Mitschrieb der Vorlesung

Darstellungstheorie I

Wintersemester 2009/10
Prof. Dr. Richard Dipper

26. Januar 2010

Mitgeschrieben von Stefan Bühler

Inhaltsverzeichnis

I. Unknown

1. Unknown

2. Gruppenkonstruktionen und Automorphismen

Definition: Sei X eine Menge. Die Freie Gruppe $\mathbb{F}X$ über X wird wie folgt konstruiert:
Ein Wort in $\mathbb{F}X$ besteht aus einer endlichen Folge

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}, k \leq 0, \varepsilon_i \in \{-1, 1\}, x_i \in X$$

Das leere Wort ($k = 0$) wird als 1 notiert.
Ist für ein $1 \leq i < k$ in einem Wort $x_i = x_{i+1}$ und $\varepsilon_i = -\varepsilon_{i+1}$, so können wir dieses Wort verkürzen, in dem wir $x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}}$ entfernen.
Wörter, die nicht mehr verkürzt werden können, heißen unverkürzbar.
Der transitive, symmetrische und reflexive Abschluss des „Kürzens" definiert eine Äquivalenzrelation; $\mathbb{F}X$ ist als die Gruppe mit der Menge der Äquivalenzklassen dieser Relation definiert, wobei die Multiplikation durch Konkatenation der Vertreter definiert wird.
Zwei Wörter sind also äquivalent, wenn man durch Kürzen und Erweitern des einen Wortes das andere erhält.
$\mathbb{F}X$ ist Gruppe mit folgender universeller Eigenschaft:

$$\begin{tikzcd} X \arrow[r, hook, "i"] \arrow[dr, "\forall f"'] & \mathbb{F}X \arrow[d, dashed, "\exists! \hat{f}"] \\ & G \end{tikzcd}$$

, so dass $\hat{f} \circ i = f$ und $\hat{f}$ Gruppenhomomorphismus.

Definition: Man kann das freie Produkt $G * H$ über den Gruppen G und H als Wörter über dem Alphabet $G \cup H$ definieren.
Das freie Produkt hat folgende universelle Eigenschaft:
Sei $\varphi : G \times H \to A$, G, H, A Gruppen, $\varphi_{|_{G \times \{1_H\}}}$ und $\varphi_{|_{\{1_G\} \times H}}$ jeweils ein Gruppenhomomorphismus, $i : (g, h) \mapsto gh$:

$$\begin{tikzcd} G \times H \arrow[r, hook, "i"] \arrow[dr, "\forall\varphi"'] & G * H \arrow[d, dashed, "\exists!\hat{\varphi}"] \\ & A \end{tikzcd}$$
, so dass $\hat{\varphi} \circ i = \varphi$ und $\hat{\varphi}$ Gruppenhomomorphismus.

Definition: Gruppen mit Erzeugenden und Relationen: X eine Menge, $S \subseteq \mathbb{F}X$ „Relationen".
Dann ist $N :=< {}^{\mathbb{F}X}S >$ die normale Hülle von S.
$G = \mathbb{F}X/N$ die Gruppe, die von X mit den Relationen S erzeugt wird; $G :=< X \mid S >$.

Beispiele:

i) Sei $n \in \mathbb{N}, C_n = \{1, g, \dots, g^{n-1}\} =< x|x^n = 1 >$
Bem: $|X| \leq 1 \Leftrightarrow \mathbb{F}X$ ist kommutativ; $\mathbb{F}X \cong \mathbb{Z} \Leftrightarrow |X| = 1$

ii) $\sigma_n =< \{s_i \mid 1 \leq i < n\} \mid s_i s_j = s_j s_i$ für $|i - j| \leq 2, s_i^2 = 1, s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} >$

Beachte:
$T \leq S \leq \mathbb{F}X \Rightarrow U :=< {}^{\mathbb{F}X}T > \leq < {}^{\mathbb{F}X}S >=: V$
$\Longrightarrow$ 1. Iso Satz$\exists$ Epimorphismus $\mathbb{F}X/U \twoheadrightarrow \mathbb{F}X/v$

iii) Die endlichen einfachenGruppen sind (durchweg?) von 2 Elementen erzeugt.

iv) Sei G Gruppe. Wähle $X = G$, nach universeller Eigenschat $\exists!$ Epimorphismus $\mathbb{F}G \twoheadrightarrow G$ mit Kern $N \Rightarrow G = \mathbb{F}G/N$

Definition: Seien G, H Gruppen. Das direkte Produkt $G \times H$ ist das kartesische Produkt mit komponentenweiser Multiplikation.
$G \cong \tilde{G} := G \times \{1_H\} \trianglelefteq G \times H \trianglerighteq \{1_G\} \times H =: \tilde{H} \cong H$
$forallg \in \tilde{G}, h \in \tilde{H} : gh = hg \Rightarrow \tilde{G}\tilde{H} = \tilde{H}\tilde{G} = G \times H, \tilde{G} \cap \tilde{H} = \{1_{G \times HJ}\}$
$\Rightarrow$ Wir müssen nicht zwischen exterem und internem Produkt unterscheiden.
$|G \times H| = |G||H|$

Betrachte $H, N \leq G, N \trianglelefteq G \Rightarrow HN = NH, HN \leq G$
Sei zusätzlich $HN = G, H \cap N = \{1\}$
Sei $n \in N$. Wegen $nHn^{-1} = H$ ist $c_n : H \to H : h \mapsto {}^nh = nhn^{-1}$ ein Automorphismus von H.
$n \mapsto c_n$ ist Gruppenhomomorphismus $N \to \mathrm{Aut}(H)$.

Satz 1.1.2.1: Sei $g \in G, c_g : G \to G : h \mapsto {}^gh$ Automorphismus von G. Die Menge $\mathrm{Inn}(G) := \{c_g \mid g \in G\} \subseteq \mathrm{Aut}(G)$ ist Normalteiler von $\mathrm{Aut}(G)$.

$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ (Gruppe der äußeren Automorphismen von G)
Die Abbildung $c : G \to Aut(G) : g \mapsto c_g$ ist Gruppenhomomorphismus mit Bild $\mathrm{Inn}(G)$ (klar) und $\ker c = Z(G) := \{g \in G \mid gh = hg \forall h \in G\}$
Also ist $G/Z(G) \cong \mathrm{Inn}(G)$

Beweis. Sei $g, h_1, h_2 \in G$
$c_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = c_g(h_1)c_g(h_2)$
$c_{g^{-1}} \circ c_g(h) = g^{-1}ghg^{-1}g = 1h1^{-1} = c_1(h) = id_H$
Also ist c_g bijektiv und daher Automorphismus von G.

$c : g \to \mathrm{Aut}(G)$ ist Homomorphismus:
$c_{g_1} \circ c_{g_2}(h) = g_1g_2hg_2^{-1}g_1^{-1} = g_1g_2h(g_1g_2)^{-1} = c_{g_1g_2}(h)$

$$\begin{aligned} c_g = id_G &\Leftrightarrow c_g(h) = h \forall h \\ &\Leftrightarrow ghg^{-1} = h \forall h \\ &\Leftrightarrow gh = hg \forall h \\ &\Leftrightarrow g \in Z(G) \\ &\Rightarrow \ker c = Z(G) \end{aligned}$$

Da $\operatorname{im} c = \mathrm{Inn}(G)$ ist $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.
Sei $\varphi \in \mathrm{Aut}(G), g \in G$: Zu zeigen: $\varphi \,\mathrm{Inn}(G) \varphi^{-1} = \mathrm{Inn}(G) \Leftrightarrow \varphi c_g \varphi^{-1} \in \mathrm{Inn}(G) \forall g, \varphi$
$(\varphi c_g \varphi^{-1})(h) = \varphi(g\varphi^{-1}(h)g^{-1}) = \varphi(g)h\varphi^{-1}(g) = \varphi(g)h\varphi(g)^{-1} = c_{\varphi(g)}(h) \forall h \in G$
$\Rightarrow \varphi c_g \varphi^{-1} = c_{\varphi(g)} \in \mathrm{Inn}(G)$
Also ist $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ □

Beachte: Sei $N \leq G$. Dann ist $N \trianglelefteq G \Leftrightarrow c_g(N) = N \forall g \in G$
($\Rightarrow c_{g_{|N}} \in \mathrm{Aut}(N)$. c_g ist $\in \mathrm{Inn}(N) \Leftrightarrow \exists n \in N : c_g = c_n$)
Definition: Sei $H < G$. Dann ist H charakteristisch in G, falls $\varphi(H) = H \forall \varphi \in Aut(G)$.
Klar: H char. in $G \Rightarrow H \trianglelefteq G$.

Beispiel:
$Z(G)$ ist char. in G:
$\forall z \in Z(G), g \in G : \varphi(g)\varphi(z) = \varphi(gz) = \varphi(zg) = \varphi(z)\varphi(g)$
$\Rightarrow \varphi(z)G = G\varphi(z)$
$\Rightarrow \varphi(z) \in Z(G)$

Satz 1.1.2.2: Seien $K \leq H \leq G$, K charakteristisch in H, H char. in G. Dann ist K char. in G.

Beweis. Sei $\varphi \in \mathrm{Aut}(G)$. Zu zeigen: $\varphi(K) = K$.
$\varphi \in \mathrm{Aut}(G) \Rightarrow_{\text{H char. in G}} \varphi(H)(= H \Rightarrow_{|H} \in \mathrm{Aut}(H) \Rightarrow \varphi(K) = \varphi_{|K} = K$, da K char. in H ist. Also ist K char. in G. □

Bemerkung. Sei $S \subseteq G$ mit $S^{-1} = S$ und $\varphi(S) = \{\varphi(s) \mid s \in S\} = S$ für alle $\varphi in \mathrm{Aut}(G)$ $(\mathrm{Inn}(G))$. Dann ist $< S > \leq G$ char. (normal) in G.

Definition: Sei G Gruppe, $a, b \in G$. Dann ist $[a, b] = aba^{-1}b^{-1}$ der Kommutator von a und b $([a, b]ba = aba^{-1}b^{-1}ba = ab)$.
Die Untergruppe $G' := < [a, b] \mid a, b \in G > \leq G$ heißt Kommutatoruntergruppe von G.

Satz 1.1.2.3: Sei G Gruppe. Dann ist G' char. in G (weil $\varphi[a, b] = [\varphi[a], \varphi[b]] \forall \varphi \in \mathrm{Aut}(G)$ ebenfalls Kommutator ist, und $[a, b]^{-1} = [b, a]$).
G' ist der kleinste Normalteiler von G, so dass G/G' abelsch ist (d.h. ist $N \trianglelefteq G, G/N$ abelsch $\Rightarrow N \supseteq G'$).

Beweis. Siehe Algebra. $(\pi : G \to G/N : g \mapsto gN, \pi[a, b] = [\pi(a), \pi(b)] = \dots dG/N = N)$, □

Definition: Seien $N, H \leq G, N \trianglelefteq G, G = NH = HN, H \cap N = \{1\}$. dann heißt G (internes) semidirektes Produkt von N mit H. Wir schreiben $G = N \rtimes H$.

Beobachtungen:

a) $G/N = NH/N \cong H/_{N\cap H} \cong H$. Also ist $G/N \cong H$. Daher ist $|G| = |N||G/N| = |N| absH = |N \times H|$

b) $G = N \cdot H \Rightarrow \forall x \in G \exists n \in N \exists h \in H : x = n \cdot h$. Diese Darstellung ist eindeutig: denn seien $n_1, n_2 \in N, h_1, h_2 \in H$ und sei $n_1h_1 = n_2h_2$, so folgt $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H \Rightarrow n_2^{-1}n_1 = h_2h_1^{-1} = 1 \Rightarrow n_1 = n_2, h_1 = h_2$

c) Allgemein gilt: $H, N \trianglelefteq G, H \cap N = \{1\} \Rightarrow hn = nh \forall n \in N, h \in H$, denn seien $h \in H, n \in N \Rightarrow [n, h] = nhn^{-1}h^{-1} = \underbrace{(nhn^{-1})}_{\in H \trianglelefteq G} h^{-1} \in H \cap N = \{1\}$ (die Klammerung analog für N)
Daher: Ist $G = N \rtimes H$ und zusätzlich $H \trianglelefteq G \Rightarrow G = H \times N$ (da $n_1h_1n_2h_2 = n_1n_2h_1h_2$)

d) $G = N \rtimes H, x = n_1h_1, y = n_2h_2 \in G \Rightarrow x \cdot y = n_1h_1n_2h_2 = n_1 \underbrace{(h_1n_2h_1^{-1})}_{\in N \trianglelefteq G} h_1h_2 = (n_1{}^{h_1}n_2)(h_1h_2) = n'h'$ die eindeutige Darstellung vom Produkt $x \cdot y$ als Produkt eines Elementes aus N mit einem Element aus H.
Die Abb. $\varphi : H \to \mathrm{Aut}(N) : h \mapsto \varphi(h) = \lambda n.{}^{h}n = \varphi_n = c_{n|_N} \in \mathrm{Aut}(N)$ ist Gruppenhomomorphismus.

e) Multiplikation in G wird vollständig auf die Multiplikation in N und Multiplikation in H und auf φ zurückgeführt: $n_1h_1n_2h_2 = n_1\varphi_{h_1}(n_2)h_1h_2$

f) Ist $\varphi : H \to \mathrm{Aut}(N)$ der triviale Homomorphismus, so ist $\varphi_n = c_{n|_N} = id_N$ für alle $h \in H$, d.h. $\varphi_h(n) = hnh^{-1} = n \Leftrightarrow hn = nh$. Dann ist $H \trianglelefteq GundG \cong H \times N$.
Daher: Ist $\varphi : H \to \mathrm{Aut}(N)$ <u>nicht</u> tirivial, so kann G nicht abelsch sein. ($\varphi(h) = \varphi_h \neq id_N, h \in H, \Rightarrow n \in N : \varphi_h(n) = hnh^{-1} \neq n \Rightarrow hn \neq hn$)

Definition: Seien H, N Gruppen, und sei $\varphi : H \to \mathrm{Aut}(N) : j \mapsto \varphi(h) = \varphi_h \in \mathrm{Aut}(N)$ ein Homomorphismus.
Wir definieren das (äußere) semidirekte Produkt $G = N \rtimes H$ wie folgt:
Als <u>Menge</u> ist G einfach das kartesische Produkt $N \times H$.
Sei $n_1, n_2 \in N, h_1, h_2 \in H$:
$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \cdot \varphi_{h_1}(n_2), h_1 \cdot h_2)$

Satz 1.1.2.4: Mit obiger Multiplikation wird $G = N \times H$ zur Gruppe $N \rtimes H$ mit Einselement $1_G = (1_N, 1_H)$ und Inverser $(n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$
Seien $\tilde{N} = N \times \{1_H\} \subseteq N \times H$ und $\tilde{H} = \{1_N\} \times H \subseteq N \times H$.
Dann ist $\tilde{N} \trianglelefteq G, H \leq G, \tilde{N} \cong N, \tilde{H} \cong H$ und $G = \tilde{N} \rtimes \tilde{H}$ (intern). Für $\tilde{h} = (1_N, h) \in \tilde{H}, \tilde{n} = (n, 1_H) \in \tilde{N}, h \in H, n \in N$ ist $\tilde{h}^{-1}\tilde{n}\tilde{h} = (\varphi_h(n), 1_H)$, d.h. $c_{\tilde{n}^{-1}|_{\tilde{N}}} \leftrightarrow \varphi_h \in \mathrm{Aut}(N)$

Beweis. Übung. □

Bemerkung. Sind φ, ψ verschiedene Homomorphismen von $H \to \mathrm{Aut}(N)$, so können $N \rtimes_\varphi H, N \rtimes_\psi H$ isomorph oder nicht isomorph sein.

Beispiel. $C_n(\cong (\mathbb{Z}/_{n\mathbb{Z}}, +)) = N, H = C_2 = \{1, h\}$
$\varphi : H \in \mathrm{Aut}(C_n)$ durch $\varphi(1) = id_{C_n}, \varphi_h(x) = x^{-1}$
Die Gruppe $D_{2n} := C_n \rtimes_\varphi C_2$ heißt <u>Diedergruppe</u> der Ordnung $2n$.
D_{2n} ist die Gruppe der Symmetrien eines regelmäßigen n-Ecks; $C_n \trianglelefteq D_{2n}$ ist die Gruppe der Rotationen, $C_2 = D_{2n}/_{C_n}$ sind die Spiegelungen.
$D_{2n} =< x, y \mid x^n = y^2 = 1, yxy = x^{-1} >$

3. Operationen von Gruppen auf Mengen

Im folgenden sei: G = Gruppe, X = Menge, $\sigma_X = \{f : X \to X \mid f\text{bij. Abb.}\}$ = „symmetrische Gruppe auf X“.

Definition: Eine (Links-)Operation von G auf X ist eine (externe) Verknüpfung

$$G \times X \to X : (g, x) \mapsto gx$$

so dass gilt:

i) $1_G \cdot x = x \forall x \in X$

ii) $(gh) \cdot x = g \cdot (h \cdot x)$

Wir sagen: „G operiert auf X“ (durch Permutationen) oder kurz: „X ist G-Menge“. (Analog: Rechtsoperation: $X \times G \to X$)

Bemerkung. Ist X G-Menge, σ_X = symmetrischeGrupe auf X, so wird durch $\lambda : G \to \sigma_X : g \mapsto \lambda_g \in \sigma_X$ ein Gruppenhomomorphismus λ definiert, wobei $\lambda_g : X \to X : x \mapsto g \cdot x$; denn: Sei $g \in G : \lambda_g \lambda_{g^{-1}} : x \mapsto g(g^{-1}x) = (gg^{-1})x = 1_G x = x \forall x \in X$, also ist λ_g bijektiv und $\in \sigma_X$.
Seien $g, h \in G \Rightarrow \lambda_g \circ \lambda_h(x) = \lambda_g(\lambda_h(x)) = g \cdot (h \cdot x) = (g \cdot h) \cdot x = \lambda_{gh}(x) \forall x \in X \Rightarrow \lambda_g \lambda_h = \lambda_{gh}$, d.h. λ ist Homomorphismus.
Umgekehrt: Sei $\varphi : G \to \sigma_X$ homomorph. Dann wird durch $g \cdot x := (\varphi(g))(x)$ eine Operation von G auf X definiert, mit $\lambda = \varphi$ (Beweis: Übung).
λ heißt „die zur G-Menge X gehörende Darstellung von G“.
Also: Das Konzept der G-Mengen X ist äquivalent zum Konzept der Homomorphismen $G \to \sigma_X$.
(Im Falle der Rechtsoperation: Entweder op σ_X auch von rechts, oder die zug. Darst. $\rho : G \to \sigma_X$ ist ein Antihomomorphismus)

Beispiele: (Running Gag)

1.) σ_X operiert auf X mit Darstellung $id_{\sigma_X} : \sigma_X \to \sigma_X : \pi \mapsto \pi \in \sigma_X, \pi x = \pi(x) \forall x \in X$

2.) G operiert auf der Menge G durch Linkstranslation $g \cdot h = gh$.
Darstellung: $\lambda G \to \sigma_G : g \mapsto \lambda_g; \lambda_g : h \mapsto gh \forall h \in G$
$(|\sigma_G| = |G|!)$

3.) G operiert auf G durch Konjugation:

$$g \cdot h = {}^g h = ghg^{-1} [= c_g(h)]$$

4.) Sei $H \leq G$, $G = \dot{\bigcup\limits_{i \in I}} g_i H$
Wir definieren eine Operation von G auf der Menge G/H der Nebenklassen von H in G durch: $g(g_i H) = g_j H$ (bzw. auf $I : g\dot{i} = j$)
(Linkstranslation auf G/H, Rechtsnebenklassen $H \backslash G$ durch Rechtstranslation)
Spezialfall: $H = (I) \Rightarrow$ Operation von G auf $G/H = G/(I) = G$ aus 2.)

4.) ist die Mutter aller G-Operationen auf Mengen.

Definition: Eine Operation von G auf X heißt treu, falls gilt: Ist $gx = x \forall x \in X \Rightarrow g = 1$. Offensichtlich heißt dies für die zugehörige Darstellung $\varphi : G \to \sigma_X$, dass φ injektiv ist; denn

$gx = x \forall x \in X \Leftrightarrow (\varphi(g))(x) = x \forall x \in X \Leftrightarrow \varphi(g) = id_X \Leftrightarrow g \in \ker \varphi$
So: $\ker \varphi = \{g \in G \mid gx = x \forall x \in X\}$.

Beispiele: 1.), 2.) treu, da $g \cdot h = h \forall h \in G \Leftrightarrow g = 1$
3.) (i.A.) nicht treu. Genauer: $\ker \varphi = \ker c_? = \{g \in G \mid c_g = id_G\} = \{g \in G \mid c_g(h) = h \forall h \in G\} = \{g \in G \mid ghg^{-1} = h \forall h \in G\} = Z(G)$ Zentrum von G.

Klar: X treue G-Menge, so enthält σ_X durch die zugehörige Darstellung $\varphi : G \to \sigma_X$ eine zu G isomorphe Untergruppe.

Definition: Seien X, Y G-Mengen. Eine Abbildung $\varphi : X \to Y$ heißt G-Homomorphismus (auch G-equivariant) falls gilt:
$\forall x \in X, g \in G : \varphi(g, x) = g\varphi(x)$
Wie üblich: Epi-, Mono- und Isomorphismen.
Komposition (und Inversen falls bijektiv) sind wieder Homomorphismen.
Isosätze etc.
Also: Kategorie der G-Mengen.

Übersetzung für Darstellungen:
Seien $\varphi : G \to \sigma_X, \psi : G \to \sigma_Y$ (X, Y Mengen) Darstellungen.
Ein Morphismus von φ nach ψ ist eine Mengenabbildung $f : X \to Y$, so dass $\forall g \in G$ das folgende Diagramm kommutiert:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi(g)"'] & Y \arrow[d, "\psi(g)"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

d.h. $f \circ \varphi(g) = \psi(g) \circ f \Leftrightarrow \psi(g) \circ f \circ \varphi(g)^{-1} = f \forall g \in G$

Dies macht die Klasse der (Permutations-) Darstellungen zu einer Kategorie. Diese ist isomoprh zur Kategorie der G-Mengen (Beweis: Übung).

Ziel: Klassifikation von G-Mengen.

Definition: X, Y $G-$ Mengen:

a) Die disjunkte Vereinigung $X \dot\cup Y$ wird zur G-Menge durch $g \cdot z = \begin{cases} gx & \text{für } z = x \in X \\ gy & \text{für } z = y \in Y \end{cases}$
(„direkte Summe“, „Koprodukt“ in Kategorie der G-Mengen)

b) Das kartesische Produkt $X \times Y$ wird zu G-Menge durch $g \cdot (x, y) = (gx, gy) \forall x \in X, y \in Y, g \in G$

c) σ_X wird G-Menge durch $gZ = \{gz \mid z \in Z\}$ für $Z \subseteq X$

Definition: Sei X eine G-Menge, $x \in X$. Die Bahn (Orbit) $Gx(^Gx)$ ist $\{gx \mid g \in G\} \subseteq X$, und der Stabilisator $Stab_G(x)$ in G von x ist $\{g \in G \mid gx = x\} \subseteq G$.
Für $S \subseteq G$ ist der $Stab_G(X) = \{g \in G \mid gs \in S \forall s \in S\}$
Der Punktstabilisator von S in G ist $PStab_G(S) = \{g\ inG | gs = s \forall s \in S\} = \bigcap_{s \in S} Stab_G(s)$
Klar:

1. $Stab_G(x), Stab_G(S), PStab_G(S)$ sind Untergruppen von G.

2. Die Einschränkung von der G-Operation auf die Bahn Gx macht die Bahn Gx von x zur G-Menge.
   Wir definieren eine Äquivalenzrelation $\sim_G$ auf X durch $x \sim_G y \Leftrightarrow \exists g \in G : y = gx$
   Die Äquivalenzklasse von $x \in X$ ist die Bahn Gx.
   Konsequenz: X ist die direkte Summe der Bahnen von G auf X.

Definition: G operiert (einfach) transitiv auf X, falls nur eine Bahn existiert, d.h. $\forall x, y \in X : \exists g \in G : x = gy$.

Beispiele: von 1.3.1

A) Bahnen:

1.) G ist die einzige Bahn.

2.) $\forall h_1, h_2 \in G \exists g \in G : h_2 = gh_1 : g := h_2 h_1^{-1}$, also: G ist die einzige Bahn.

3.) $g \sim_G h \Leftrightarrow \exists x in G : h = xgx^{-1} \Leftrightarrow g$ und h sind konjugiert $\Leftrightarrow$ Bahnen sind Konjugationsklassen.

4.) Eine Bahn. $g, h \in G \Rightarrow \exists x \in G : h = xg \Rightarrow hH = xgH$

B) Stabilisatoren:

1.) $x \in X : Stab_{\sigma_X}(x) = \{\pi \in \sigma_X \mid \pi(x) = x\} = \sigma_{X \setminus \{x\}}$, z.Bsp. $Stab_{\sigma_n}(n) = \sigma_{n-1}$
$Stab_{\sigma_n}(\{1, \ldots, i\}) = \{\pi \in \sigma_n | 1 \leq \pi(j) \leq i \forall 1 \leq j \leq i\} = \sigma_{\{1,\ldots,i\}} \times \sigma_{\{i+1,\ldots,n\}}$

2.) $h \in G : Stab_G(h) = \{g \in G \mid gh = h\} = \{1\}$

3.) $h \in G : Stab_G(h) = \{g \in G \mid {}^g h = h\} = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} =$ Zentralisator von h in G.

4.) Spezialfall $Stab_G(1 \cdot H) = \{g \in G \mid gH = H\} = H$

Lemma 1.1.3.1: Sei X G-Menge, $x \in X, g \in G$: Dann ist $Stab_G(gx) = g \cdot Stab_G(x() \cdot g^{-1}$ („konjugierte Untergruppe“)

Beweis. „$\supseteq$" Sei $h = gfg^{-1} \in$ rechte Seite $\Rightarrow h(gx) = gfg^{-1}gx = gfx = gx \Rightarrow h \in$ linke Seite. „$\subseteq$" Sei $h \in Stab_G(gx)$, d.h. $h(gx) = gx \Rightarrow g^{-1}hgx = x \Rightarrow g^{-1}hx = f \in Stab_G(x) \Rightarrow h = gfg^{-1} \in gStab_G(x)g^{-1}$ □

Beispiele: von 1.3.1, Stabilisator für 4.):
$Stab_G(xH) = xHx^{-1}$

Neues Beispiel für 1.3.1:

5.) Sei $X = \{H \leq G\}$. Dann operiert G auf X durch Konjugation $lsupgH = gHg^{-1}$
$Stab_G(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ der Normalisator von H in G (die größte Untergruppe von G in der H normal ist, $H \trianglelefteq N_G(H) \leq G$)

Bemerkung. Bahnen sind in 5.) Konjugationsklassen von Untergruppen.
Beachte: $|c_g(H)| = |gHg^{-1}| = |H|$

Satz 1.1.3.2: Jede G-Menge ist (eindeutig) disjunkte Vereinigung (direkte Summe) von transitiven G-Mengen, nämlich der Bahnen von G auf der Menge.

Satz 1.1.3.3: Sei X transitive G-Menge und $x \in X, H = Stab_G(x)$. Dann ist $X \cong G/H$ (= G-Menge der Nebenklassen von H in G durch Linkstranslation, siehe Beispiel 4. aus 1.3.1)

Beweis. Definiere $\varphi : G/H \to X : gH \mapsto gx$ für $g \in G$.

1.) φ ist wohldefiniert: Denn sei $gH = fH \Rightarrow f^{-1}g \in H \Rightarrow f^{-1}gx = x$, da $H = Stab_G(x)$ ist $\Rightarrow gx = fx$

2.) Umgekehrt gehts auch: Sei $fx = gx$ $(f, g \in G) \Rightarrow x = f^{-1}gx \Rightarrow f^{-1}g \in H \Rightarrow gH = fH$
Also ist φ injektiv.

3.) Wegen $G \cdot x = X$ ist φ surjektiv.

4.) Seien $a, g \in G$: Dann ist $a\varphi(gH) = a(gx) = (ag)x = \varphi(agH)$, also ist φ ein Isomorphismus von G-Mengen.

□

Korrolar 1.1.3.4: $|X| = |G/H| = [G : H]$
Allgemein: Sei X G-Menge, $x \in X \Rightarrow |Gx| = |G : Sta_G(x)|$ (Bahngleichung)

Wir haben jetzt is aus Isomorphie alle G-Mengen konstruiert, nämlich als disjunkte Vereinigunge (direkte Summen) von G-Mengen der Form G/H mit $H \leq G$.
Frage: Sind $H, K \leq G$. Wann ist $G/H \cong G/K$ als G-Menge (unter Linkstranslation)?

Lemma 1.1.3.5: Seien X, Y G-Mengen, $\varphi : X \to Y$ Homomorphismus, und sei $x \in X$. Dann ist $\mathrm{Stab}_G(x) \leq \mathrm{Stab}_G(\varphi(x)$
Insbesondere: ist φ ein Isomorphismus, so ist $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(\varphi(x))$.

Beweis. $g \in G : gx = x \Rightarrow g(\varphi(x)) = \varphi(gx) = \varphi(x) \Rightarrow g \in \mathrm{Stab}_G(\varphi(x))$ □

Satz 1.1.3.6: Seien $H, K \leq G$. Dann ist $G/H \cong G/K \Leftrightarrow H =_G K$ (d.h. $\exists g \in G : gKg^{-1} = H$).

<u>Bemerkung:</u> 1.3.6 + 1.3.9 liefert die Klassifikation der G-Mengen.

Beweis. Sei $\varphi : G/H \to G/K$ ein Isomorphismus von G-Mengen, $(\exists x \in G) : varphi(1 \cdot H) = xK \Rightarrow \mathrm{Stab}_G(1 \cdot H) = H = \mathrm{Stab}_G(xK) = x\,\mathrm{Stab}_G(1 \cdot K)x^{-1} = xKx^{-1}$. Also ist $H =_G K$.
Umgekehrt ist $H =_G K$, etwa $K = xHx^{-1}$. Dann ist (nach 1.3.4) $K = \mathrm{Stab}_G(xH)$, und $G/K \cong G/H$ nach 1.3.6 □

Definition: Sei $k \in \mathbb{N}, X$ G-Menge. Dan heißt X k-fach transitiv (k-trans.) falls gilt: Sind $x_1, \ldots, x_k \in X$ und $y_1, \ldots, y_k \in X$ jeweils beliebige aber paarweise verschieden, so gibt es $g \in G : y_i = gx_i \forall 1 \leq i \leq k$
(Klar: G operiert auf $X^{\times k} = X \times \ldots \times X$ k-trans. $\Leftrightarrow$ G operiert auf $\{(x_1, \ldots, x_k) \in X^{\times k} \mid x_i$ paarweise vers
transitiv. 1-transitiv = transitiv)
Satz 1.1.3.7: Sei X 2-transitive G-Menge, $x \in X$. Dann ist $\mathrm{Stab}_G(x)$ maximale Untergrupe von G.

Beweis. 2-transitiv $\Rightarrow$ X ist transitiv $\Rightarrow$ $X \cong G/H$ für $H = \mathrm{Stab}_G(X)$. Angenommen, H st nicht maximal in G. Sei $H < K < G, g \in G, g \notin K, k \in K, k \notin H$. Dann ist $kH \neq H, gH \neq H$. Wir hben also zwei Paare (H, kH) und (H, gH). 2-transitiv $\Rightarrow \exists f \in G : f \cdot (1H) = (1H), f(kH) = gH \Rightarrow f \in H \Rightarrow fk \in K \Rightarrow \exists h \in H : fk = gh \Rightarrow K = fkK = ghK = gK \Rightarrow g \in K$ Widerspruch! □

Definition: Eine transitive G-Menge X heißt primitiv $\Leftrightarrow$ $\forall x \in X : \mathrm{Stab}_G(x)$ maximale Untergruppe von G ist.

$$\begin{array}{ccccc}
\text{2-transitiv} & \Rightarrow & \text{„primitiv“} & \Rightarrow & \text{transitiv} \\
\Downarrow & & \Updownarrow & & \Updownarrow \\
\text{Stab = max. Untergruppe} & & \text{Stab = max. Untergr.} & & \text{Stab = bel. Untergr.}
\end{array}$$

Satz 1.1.3.8: Eine transitive G-Menge X ist primitiv $\Leftrightarrow$ wenn gilt: Sei $Y \subsetneq X, |Y| \geq 2$. Dann gibt es für alle $g \in G$ Elemente $y, z \in Y$ mit $gy \in Y, gz \notin Y$.

Anwendungen:

Satz 1.1.3.9: Sei G endlich, $H, K \leq G$. Es gilt:

$$|H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Beweis. Sei $X = G/K$ eine G-Menge. Durch Einschränken ist G/K auch H-Menge.
Sei H_K die Bahn von $K = 1 \cdot K$ unter dieser H-Operation.
Klar: $H_K = \{hK \mid h \in H\}, HK = \bigcup\limits_{h \in H} hK$.
Also ist HK die Vereinigung von K-Nebenklassen von G mit Vertretern aus H.
Also ist $|HK| = |{}^H K| \cdot |K|$. Nach 1.3.7 ist $|{}^H K| = |H : \mathrm{Stab}_H(K)|$
$\mathrm{Stab}_H(K) = \{h \in H \mid hK = K\} = K \cap H$.
Also ist $|HK| = |K| \cdot |{}^H K| = |K| \cdot |H : \mathrm{Stab}_H(K)| = |K| \cdot |H : (H \cap K)| = |K| \cdot \frac{|H|}{|H \cap K|}$ □

Konjugationsop: $|G| = n \in \mathbb{N}, 1 = g_1, g_2, \ldots, g_k$ seien Vertreter der Konjugationsklassen von G.
$\mathcal{C}_i := {}^G g_i = \{g g_i g^{-1} \mid g \in G\}$ Bahn
$C_i = \mathrm{Stab}_G(g_i) = C_G(g_i) = \{h \in G \mid hg_i = g_i h\} \leq G$

Satz 1.1.3.10: Klassengleichung: Sei $|G| = n$.
$n = 1 + \sum_{i=2}^k |G : C_i| = |Z(G)| + \sum\limits_{i=1,\ldots,k, g_i \notin Z(G)} |G : C_i|$

Beweis. Ohne Einschränkung: $Z(G) = \{g_1, \ldots, g_l\}, 1 \leq l \leq k \Rightarrow C_i = G \forall i = 1, \ldots, l, \mathcal{C}_i = \{g_i\}$
Mit 1.3.7 $\underset{i=1,\ldots,k}{\Rightarrow} |{}^G g_i| = |\mathcal{C}_i| = [G : C_i] = [G : \mathrm{Stab}_G(g_i)]$ □

Definition: Sei G endliche Gruppe, $G^1 = [G, G]$. Definiere $D^i(G) (i \in \mathbb{N})$ durch

1. $D^1(G) = G^1$
2. $i > 1 : D^i(G) = [D^{i-1}(G), D^{i-1}(G)]$

Klar: $D^i(G) \trianglelefteq D^{i-1}(G)$ und $D^{i-1}(G)/D^i(G)$ abelsch.
G heißt auflösbar, falls $D^k(G) = (1)$ für ein $k \in \mathbb{N} \Leftrightarrow \exists (1) = N_1 \leq N_2 \ldots \leq N_m = G$ mit $N_i \trianglelefteq N_{i+1}$ und N_{i+1}/N_i abelsch (zyklisch, zyklisc von Primzahlordnung nach Korrespondenzsatz).
Kann man zusätzlich N_i so wählen, dass $N_i \trianglelefteq G$ ist, so heißt G Überauflösbar („supersolvable").
$N \trianglelefteq G$: mit N auflösbar, G/N auflösbar $\Leftrightarrow G$ auflösbar.

Sei $Z_i(G)$ induktiv durch folgendes definiert:

i) $Z_1(G) = Z(G) \trianglelefteq G$ (charakteristisch)

ii) $Z_2(G)$ ist volles Urbild von $Z(G/Z(G))$ in G unter natürlicher Projektion $G \to G/Z(G)$.
Beachte: Nach Korrespondenzsatz (1.2.10) gilt: $Z_2(G) \trianglelefteq G$.
$(Z_2(G) = \{g \in G \mid gZ(G) \in Z(G/Z(G))\})$

iii) $i > 1 : Z_i(G)$ ist volles Urbild von $Z(G/Z_{i-1})$ in $G, Z_i(G) \trianglelefteq G$.

Haben: $(1) = Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \ldots \trianglelefteq Z_i(G) \trianglelefteq \ldots$
$Z_i(G)/Z_{i-1}(G)$ abelsch, $Z_i(G) \trianglelefteq G$. (Beweis: Übung)
G heißt nilpotent, falls $\exists k \in \mathbb{N} : Z_k(G) = G$.
Beachte: nilpotent $\Rightarrow$ überauflösbar $\Rightarrow$ auflösbar

Korrolar 1.1.3.11: Sei G eine p-Gruppe, p Primzahl (d.h. $\exists t \in \mathbb{N} : |G| = p^t$), Dann ist $|Z(G)| > 1$.
Insbesondere ist G nilpotent.

Beweis. $x \in G, x \notin Z(G) \Rightarrow C_G(x) \lneq G \Rightarrow [G : C_G(x)]$ wird von p geteilt.
Klassengleichung: $|G| = p^t = |Z(G)| + \sum\limits_{i=l+1}^{k} |G : C_G(g_i)|$
p teilt $|G : C_G(g_i)| \Rightarrow p$ teilt die Summe $\Rightarrow p$ teilt $|Z(G)|$.
Rest: Übung. □

Bemerkung. Berühmte Ergebnisse:

I) Brunside's pq-Theorem: Seien p, q Primzahlen, $|G| = p^a \cdot q^b, a, b \in \mathbb{N} \Rightarrow G$ ist auflösbar.

II) Feit-Thompson: Ist $2 \nmid |G| \Rightarrow G$ ist auflösbar.

Beachte: Sei $H \leq G$. Dann ist $H \trianglelefteq G \Leftrightarrow H$ ist Vereinigung von (disjunkten) Konjugationsklassen von G; denn $gHg^{-1} = H \forall g \in G$ gilt genau dann, wenn $\forall h \in H, g \in G : c_g(h) = ghg^{-1} \in H$, d.h. ${}^G h \subseteq H$. Daher ist $|H| = \sum\limits_{g_i \in H} |C_i|$

Erinnerung: Sei $H \leq G$. Dann ist $N_g(H) = \{g \in G \mid gHg^{-1} = H\} \leq G$ und $H \trianglelefteq N_G(H) =$ die eindeutig bestimmte größte Untergruppe von N, in der H normal ist. $H \trianglelefteq G \Leftrightarrow N_G(H) = G$.

Satz 1.1.3.12: Sei $|G| = n < \infty$, und sei $H \leq G$. Sei $\mathcal{A} = \{gHg^{-1} \mid g \in G\}$. Dann ist $|\mathcal{A}| = |G : N_G(H)|$.

Beweis. G operiert auf $\sigma(G)$ $(\{K \leq G\})$ per Konjugation, und $\mathcal{A}$ ist gerade die Bahn ${}^G H$ von H unter dieser Operation. $N_G(H) = \mathrm{Stab}_G(H)$. So folgt die Behauptung aus 1.3.7. □

Definition: $H, K \leq G, z \in G$. Dann heißt $HzK = \{hzk \mid h \in H, k \in K\}$ die H-K-Doppelnebenklasse von z.
Definiere $\sim$ auf G durch $, y \in G$, so ist $x \sim y \Leftrightarrow \exists h \in H, k \in K : y = hxk$

i) $x = 1_H x 1_K \Rightarrow x \sim x \forall x \in G$

ii) $y = hxk \Rightarrow x = h^{-1} y k^{-1} \Rightarrow$ Symmetrie

iii) $y = h_1 x k_1, z = h_2 y k_2 \Rightarrow z = h_2 h_1 x k_1 k_2 \Rightarrow x \sim z$

Also ist G disjunkte Vereinigung der H-K-Doppelnebenklassen.

Klar: $HzK = \bigcup_{h \in H} hzK = \bigcup_{k \in K} Hzk$ ist (disjunkte) Vereinigung von K-Links- bzw H-Rechtsnebenklassen in G.
Satz 1.1.3.13: Sei $|G| = n < \infty, H, K \leq G$ und $\in G$. Dann gilt:

$$|HzK| = \frac{|H| \cdot |K|}{|H \cap zKz^{-1}|} = \frac{|H| \cdot |K|}{|z^{-1}Hz \cap K|} = [H : (H \cap zKz^{-1}] \cdot |K| = |H| \cdot [K : (z^{-1}Hz \cap K]$$

Das kommt nicht von unefähr: Ist $h_1 = 1, h2, \ldots, h_l \in H$ ein Vertretersystem der Linksnebenklassen von $H \cap zKz^{-1}$ in H, d.h. $H = \dot{\cup} h_i (H \cap zKz^{-1}$, so ist $HzK = \dot{\bigcup}_{j=1,\ldots,l} h_i zK$.
Analog $K = \dot{\bigcup}_{j=1,\ldots,m} (z^{-1}Hz \cap K) \cdot k_j, HzK = \dot{\bigcup}_{j=1,\ldots,m} Hzk_j$

Beweisidee: $h \in H \cap zKz^{-1} \Leftrightarrow \exists k \in K : h = zkz^{-1} \Leftrightarrow hzK = zkz^{-1}zK = zkK = zK \Rightarrow h_i(z^{-1}H \cap K)zK = h_i zK$, Details Übung.

Beweis. a) $|HzK| = |HzKz^{-1}| \overset{1.3.12}{=} \frac{|H| \cdot |zKz^{-1}|}{|H \cap zKz^{-1}|} = \frac{|H| \cdot |K|}{|H \cap zKz^{-1}|} = \frac{|H| \cdot |K|}{|z^{-1}Hz \cap K|}$

b) 2. Beweis: G operiert auf G/K wie üblich, also auch H durch Einschränkung. HzK ist die Vereinigung der Nebenklassen, die in ${}^H zK$ liegen. Daher ist $|HzK| = |K| \cdot$ Bahnlänge $|{}^H zK|$. Nun ist $\mathrm{Stab}_H(zK) = \{h \in H \mid hzK = zK\}$. Aber $hzK = zK \Leftrightarrow z^{-1}hz = k \in K \Leftrightarrow h = zkz^{-1}$ ist $\exists k \in K$.
Also ist $\mathrm{Stab}_H(zK) = H \cap zKz^{-1} \overset{1.3.7}{\Rightarrow} |HzK| = |K|[H : H \cap zKz^{-1}] = \frac{|H| \cdot |K|}{|H \cap zKz^{-1}|}$

□

F ist ein Körper, $n \in \mathbb{N}, G = \mathrm{GL}_n(F) \cong \mathrm{Aut}_F(V), v = F$-Vektorraum mit $\dim_F(V) = n$
$G = \{A \in F^{n \times n} \mid \det A \neq 0\}$ = volle lineare Gruppe.
$SL_n(F) = \{A \in F^{n \times n} \mid \det A = 1\}$ = spezielle lineare Gruppe.
$Z(G) = \{\alpha \cdot E_{n \times n} | 0 \neq \alpha \in F\}$

$Z(\mathrm{SL}_n(F)) = Z(G) \cap \mathrm{SL}_n(G)$, da $G = \mathrm{SL}_n(F) \cdot \left\{ \begin{pmatrix} \alpha & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \right\}$

$Z(\mathrm{SL}_n(F)) = \{\alpha \cdot 1_G \mid 0 \neq \alpha \in F, \alpha^n = 1\}$
$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$ = „projektive spezielle lineare Gruppe“
Ziel: $\Gamma = \mathrm{PSL}_n(F), \Gamma \neq \mathrm{PSL}_n(\mathrm{GF}(q))$ für $n = 2, q = 2, 3$ und $n = 3, q = 2$, dann ist $\mathrm{PSL}_n(F)$ einfach.

Notation: $|F| = \mathrm{GF}(q) = \mathbb{F}_q$ Körper mit q Elementen, $q = p^a, p$ Primzahl, $a \in N$.
$G = \mathrm{GL}_n(q), \mathrm{SL}_n(F) = \mathrm{SL}_n(q), \mathrm{PSL}_n(F) = \mathrm{PSL}_n(q)$
$|G| = \prod_{k=1}^{n} (q^n - q^{k-1}) = (q^n - 1)(q^n - q)(q^n - q^2) \ldots = q^{\frac{n(n-)}{2}} (q^n - 1)(q^{n-1} - 1) \ldots (q - 1)$
$|\mathrm{SL}_n(q)| = \frac{|\mathrm{GL}_n(q)|}{q-1}, |\mathrm{PSL}_n(q)| = \frac{|\mathrm{SL}_n(q)|}{|\alpha|\alpha^n = 1 \in F|}$

II. Basics und Bruhat-Zerlegung

Satz 1.2.14: $|\mathrm{GL}_n(q)| =$ oben (Algebra)
Definition: $T := \{\text{Diagonalmatrizen in } G = diag(\alpha_1, \dots, \alpha_n) \mid 0 \neq \alpha_i \in \mathbb{F}_q\}, |T| = (q-1)^n$, Standard (Split) „Torus“
$B := \{A = \text{obere Dreiecksmatrizen in } G \mid \det A = \prod \alpha_i \neq 0\}$, Standard „Boreluntergruppe“ von G
Klar: $T \leq B \leq G$ „Borus“, „Torel“; $A \in B \Rightarrow A^{-1} \in B; X, Y \in B \Rightarrow XY \in B$, also $B \leq G$.
$U = \{A \in B \mid \text{Diagonaleinträge von } A \text{ sind } 1\} \leq B$
$A \in B, X \in U : AXA^{-1} \in U \Rightarrow U \trianglelefteq B$

Klar: $U \cap T = (1_G)$.

Sei $A =\in B \Rightarrow A \cdot \begin{pmatrix} A_{11}^{-1} & & 0 \\ & \ddots & \\ & & A_{nn}^{-1} \end{pmatrix} \in U$

d.h. $Y \in T, A \cdot Y = X \Rightarrow A = X \cdot Y^{-1}$. Also ist $B = U \cdot T$.

Definition: i) Eine Untergruppe von G, die konjugiert zu B ist, heißt Boreluntergruppe von G.

ii) Sei $\xi = (e_1, \dots, e_n)$ natürliche Basis von $\mathbb{F}_q^n$, Für $\pi \in \sigma_n$ sei $\xi_\pi = (e_{\pi(1)}, \dots, e_{\pi(n)})$.
Sei $E_\pi = m_{\mathrm{id}}(\xi, \xi_\pi)$ Basiswechselmatrix von ξ nach ξ_π

Beispiel: $\pi = (2, 3, 1) : E_\pi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} =$ Permutationsmatrix zu π.

Beachte: Matrix-Einheit: $e_{ij} = (\delta_{rs}) \in M_{n \times n}(\mathbb{F}_q)$

$E_\pi = \sum\limits_{i=1}^{n} e_{\pi(i)i}$

Definition: Eine Permutationsmatrix $A \in M_{n \times n}(F)$ ist eine Matrix, die in jeder Spalte und Zeile genauen einen von 0 verschiedenen Eintrag hat, der 1 ist.
Sei A Permutationsmatrix. Definiere $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ durch $\pi(i) = j \Leftrightarrow A_{\pi(i)j} = 1$.

Also ist $\pi \mapsto E_\pi$ eine Bijektion von σ_n in $W := \{\text{Permutationsmatrizen}\}$.

Seien $\sigma, \pi \in \sigma_n$. Dann ist $E_\pi \cdot E_\sigma = (\sum_{i=1}^n e_{\pi(i)i})(\sum_{j=1}^n e_{\sigma(j)j}) = \sigma_{i,j} e_{\pi(i)i} e_{\sigma(j)j} = \sum_{j=1}^n e_{\pi\sigma(j)j} =$

$E_{\pi\sigma}$.
Also ist $\pi \mapsto E_\pi$ ein Isomorphismus von σ_n in W, insbesondere ist $W \leq G$, W heißt „Weylgruppe“ von G.

Satz 1.2.15: Die Menge W der Permutationsmatrizen in $G = \mathrm{GL}_n(F)$ ist Untergruppe von G und isomorph zu σ_n.
Beachte: Sei $\pi \in W \Rightarrow \det \pi = \operatorname{sign} \pi \in \{-1, +1\}$

Bemerkung. Ist E_π Permutationsmatrix zu $\pi \in \sigma_n, M \in F^{n\times n}$, so entsteht $\pi \cdot M = E_\pi M$ aus M durch entsprechende Zeilenpermutationen und $M\pi$ durch entsprechende Spaltenpermutationen.
σ_n operiert auf der natürlichen Basis $\xi \rightsquigarrow \xi_\pi = (e_{\pi(1)}, \ldots, e_{\pi(n)})$.

Definition: Sei $1 \leq i, j \leq n, i \neq j$, und sei $\alpha \in F$. Dan sei $x_{ij}(\alpha) \in F^{n\times n}$ die entsprechende Elementarmatrix $A = (\alpha_{st})$ mit $\alpha_{st} = \begin{cases} 1 & \text{für } s = t \\ \alpha & \text{für } s = i, t = j \\ 0 & \text{sonst} \end{cases}$

$x_{ij}(\alpha) = \begin{pmatrix} 1 & & \alpha \\ & \ddots & \\ & & 1 \end{pmatrix}$, α an Position i, j

Die Matrizen $x_{ij}(\alpha)$ und ihre G-konjugierten heißen Transvektionen.
Beachte: $x_{ij}(\alpha) \cdot M$ entsteht aus M durch Addition von Reihe (Saplte) j mal α zu Zeile (Spalte) i ($M \cdot x_{ij}(\alpha)$.

Lemma 1.2.16: Seien $\alpha, \beta \in F, i \neq j, \pi in W$

i) $\det(x_{ij}(\alpha)) = 1$, also ist $x_{ij}(\alpha) \in \Omega_n(F) \leq \mathrm{GL}_n(F)$.

ii) Ist $\alpha \neq 0$, so ist $x_{ij}(\alpha) \in B \Leftrightarrow i < j$. ($U \leq B$)

iii) $x_{ij}(\alpha)x_{ij}(\beta) = x_{ij}(\alpha+\beta), x_{ij}(\alpha)^{-1} = x_{ij}(-\alpha)$. So ist $X_{ij} = \{x_{ij}(\alpha) \mid \alpha \in F\} \leq G$ die sogenannte Wurzeluntergruppe zur Wurzel $(j - i)$; $X_{ij} \cong (F, +)$

iv) Sind $i, j, k \in \{1, \ldots, n\}$ paarweise verschieden, so ist $[x_{ij}(\alpha), x_{jk}(\beta)] = x_{ik}(\alpha\beta)$

v) Ist $\pi \in \sigma_n$, so ist $\pi x_{ij}(\alpha)\pi^{-1} = x_{\pi(i)\pi(j)}(\alpha)$

vi) Bemerkung von oben.

Beweis. i),ii) trivial.

iii) Beachte: $x_{ij}(\alpha) = E + \alpha e_{ij}$
$(E + \alpha e_{ij})(E + \beta e_{ij}) = E + (\alpha+\beta)e_{ij} + \alpha\beta e_{ij}e_{ij} = E + (\alpha+\beta)e_{ij} = x_{ij}(\alpha+\beta)$.
$\Rightarrow x_{ij}(\alpha) \cdot x_{ij}(-\alpha) = x_{ij}(0) = E = 1 \Rightarrow x_{ij}(\alpha)^{-1} = x_{ij}(-\alpha)$

iv) $[x_{ij}(\alpha), x_{jk}(\beta)] = (E + \alpha e_{ij})(E + \beta e_{jk})(E - \alpha e_{ij})(E - \beta e_{jk})$
$= (E + \alpha e_{ij} + \beta e_{jk} + \alpha\beta e_{ik}) \cdot (E - \alpha e_{ij} - \beta e_{jk} + \alpha\beta e_{ik})$
$= E - \alpha e_{ij} - \beta e_{jk} + \alpha\beta e_{ik} + \alpha e_{ij} - 0 - \alpha\beta e_{ik} + 0 + \beta e_{jk} - 0 + 0 + \alpha\beta e_{ik} - 0 - 0 + 0$
$= E + \alpha\beta e_{ik} = x_{ik}(\alpha \cdot \beta)$

v) Beachte: $\pi e_{ij} = e_{\pi(i)j}$ wegen vi). $e_{ij}\pi^{-1} = e_{i\pi(j)}$; denn $E_\pi = \sum\limits_{s=1}^{n} e_{\pi(s)s}$
$\Rightarrow E_\pi e_{ij} = \sum\limits_{s=1}^{n} e_{\pi(s)s} e_{ij} = e_{\pi(s)j}, e_{ij}E_{\pi^{-1}} = \sum e_{ij}e_{\pi^{-1}(s)s} = e_{i\pi(j)}$
$\Rightarrow \pi x_{ij}(\alpha)\pi^{-1} = \pi(E + \alpha e_{ij})\pi^{-1} = \pi E \pi^{-1} + \alpha\pi e_{ij}\pi^{-1} = E + \alpha e_{\pi(i)\pi(j)} = x_{\pi(i)\pi(j)}(\alpha)$

□

<u>Ziel:</u> $G = \dot{\bigcup\limits_{w \in W}} BwB$, insbesondere: es gibt $n!$ viele B-B-Doppelnebenklassen in G (U-B-, B-U-). „Bruhat-Zerlegung“

Lemma 1.2.17: Sei $M \in G$. Dann gibt es ein $b \in B(U)$ so, dass gilt:
Für $1 \leq i \leq n$ gibt es eine eindeutig bestimmte Zeile k_i in $b \cdot M$ so, dass der i-te Eintrag in dieser Zeile der erste von 0 verschiedene Eintrag in ihr ist,
und $\{k_1, \dots, k_n\} = \{1, \dots, n\}$; $i \mapsto k_i \in \sigma_n$.

Beweis. Die 1. Spalte von M kann nicht die 0-Spalte sein $\Rightarrow \exists k_1$ so, dass Eintrag k_i in $M = (\alpha_{rs})$ ungleich 0 aber $\alpha_{r1} = 0$ für $r > k_1$ ist. (Der letzte von 0 verschiedene Eintrag in der Spalte).
Durch elementare Zeilentransformationen ($x_{1,l}(\frac{-\alpha_{l,1}}{\alpha_{k_1 1}})$, $l < k_1$) aus U kann man M' erhalten, in der k_i der einzige von 0 verschiedene Eintrag in der 1. Spalte ist.
Streiche 1. Spalte und k_1-te Zeile und arbeite induktiv weiter. □

Satz 1.2.18: $G = BWB = \bigcup\limits_{w \in W} BwB$ (bzw. UwB oder BwU).

Beweis. $M \in G, b \in B, k_i$ wie in 2.1.5 gewählt. Die Abbildung $i \mapsto k_i$ ist Permutation $\pi = \pi_M \in \sigma_n$.
Sei $w = \pi^{-1}$. Dann ist $wbM = \tilde{b} \in B \Rightarrow M = b^{-1}\pi\tilde{b} \in B\pi B$.
<u>Beachte:</u> 2.1.5 konstruiert π_M für M. □

Lemma 1.2.19: Seien $w_1, w_2 \in W$ und $b \in B$, so dass $w_1 b w_2 \in B$ ist, dann ist $w_1^{-1} = w_2$.

Beweis. Sei $1 \leq j \leq n$ beliebig und sei $i = w_1^{-1}(j)$, also $w_1(i) = j$.
Sei wieder $E = (e_1, \dots, e_n)$ natürliche Basis von F^n,so ist ${}_1^{-1}(e_j) = e_i$.
Dann ist Zeile j von $w_1 b$ gleich Zeile i von b.
Sei $k = w_2^{-1}(i)$, d.h. $w_2(k) = i$, dann ist Spalte k von $w_1 b w_2$ gleich Spalte i von $w_1 b$.
Es sei $\beta = (b)_{ii} \in F$. $\beta \neq 0$ ($b \in B$); β ist auch $(w_1 b)_{ji}$ und $(w_1 b w_2)_{jk}$ (und immer noch $\neq 0$)

$\Rightarrow j \leq k$, da $w_1 b w_2 \in B$
Wir haben $w_2^{-1} w_1^{-1}(j) = w_2^{-1}(i) = k \geq j \Rightarrow w_2^{-1} w_1^{-1} = 1 \Rightarrow w_1 = w_2^{-1}$ $\square$

Korrolar 1.2.20: Seien $w, w' \in W, w \neq w'$. Dann ist $BwB \cup Bw'B = \emptyset$, und daher $G = \dot{\bigcup\limits_{\pi \in W}} B\pi B$.

Beweis. Sei $BwB \cap Bw'B \neq \emptyset \Rightarrow BwB = Bw'B \Rightarrow \exists b, b' : w' = bwb'$
$\Rightarrow w^{-1} b^{-1} w' = b' \in B \Rightarrow w^{-1} = (w')^{-1} \Rightarrow w = w'$ $\square$

Bemerkung. In 2.1.5 wird das eindeutig bestimmte $w \in W$ für $M \in G$ konstruiert so, dass $M \in BwB$ ist.

Lemma 1.2.21: Sei $b \in B$. Dann gibt es ein Produkt t von Transvektionen so, dass $t \cdot b$ Diagonalmatrix ist, die dieselben Diagonaleinträge wie b hat.
Beweis klar.

Satz 1.2.22: G wird von $T \leq G$ und der Menge der Transvektionen erzeugt.

Beweis. Sei H die Untergruppe von G, die von diesen Matrizen erzeugt wird.
Zu zeigen: $H = G$
Wegen 2.1.10 ist $B \leq H$, und daher genügt es wegen der Bruhat-Zerlegung 2.1.8 zu zeigen, dass $w \in H \forall w \in W$.
Dafür genügt es zu zeigen: $\tau_{i,j} \in \sigma_n$ ist in H enthalten:
$E_{\tau_{i,j}} = \sum\limits_{s \neq i, s \neq j} e_s s + e_i j + e_j i = x_{ji}(1) x_{ij}(-1) x_{ji}(1) \cdot D, D$ Diagonalmatrix.

$$w = x_{ji}(1) x_{ij}(-1) x_{ji}(1), w e_k = \begin{cases} e_n & \text{für } k \neq i, k \neq j \\ e_j & \text{für } k = i \\ -e_i & \text{für } k = j \end{cases}$$ $\square$

Missing: 17.11.2009

$P_f = U_f \rtimes L_f$

<u>Beispiele:</u> $V = F^n, \xi = (e_i, \ldots, e_n), V_i =< e_i, \ldots, e_{n_i} >, 0 < n_1 < \ldots < n_k = nf = (V_1, \ldots, v_n)$
<u>Beachte:</u> $V_i = V_{i-1} \oplus y_i, y_i := < e_{n_i+1}, \ldots, e_{n_i} >$
$v_i = n_i, v_2 = n_2 - n_1, v_3 = n_3 - n_2, \ldots, v_k = n_k - n_{k-1}, v_i = \dim_F(y_i)$
$L_f = \{$Matrix mit von 0 verschiedenen Blöcken der Größen $v_i \times v_i$ auf der Diagonale aus $G\}$
...

$v = (v_1, \ldots, v_k) \models n$ Wir schreiben $P_v = U_v \rtimes L_v$ anstatt P_f, L_f, U_f. $(\nu = (n) \Rightarrow P_{(n)} = G = L_{(n)}, U_{(n)} = (1))$
<u>Sonderfall:</u> $v = (1^n) = (1, \ldots, 1) \models n, P_v = B = u \cdot T$, Borus.

Definition: Eine $n \times m$-Matrix A heißt (untere) unitriangulär, falls folgendes gilt: $A_{ii} = 1, A_{ij} = 0 \forall i < j$ (allgemeine untere Dreiecksmatrix mit 1 auf der Diagonale), analog obere.

Lemma 1.2.23: Sei $V = F^n, f = (W_1, \ldots, W_n)$ mit $W_i =< e_1, \ldots, e_i >, \xi = (e_1, \ldots, e_n)$ natürliche Basis von V.
Sei X ein B-invarianter Unterraum von V, d.h. $bx \in X \forall b \in B, x \in X (\Rightarrow bX = X$.
Dann ist $W = W_i$ für ein $1 \leq i \leq n$.

Beweis. Sei $1 \leq k \leq n$ minimal mit $X \subseteq W_k$. Wir zeigen: $X = W_k$.
Dann existiert ein $x = \sum\limits_{i=1}^{k} \alpha_i e_i$ mit $\alpha_k \neq 0$ (da k minimal).
... $\exists b \in B : b \cdot x = e_k \Rightarrow e_k \in X$
Nun ist $(E + e_{k-1,k})e_k = e_k + e_{k-1} \in X \Rightarrow e_{k-1} \in X$, analog $\forall i \leq k : e_i \in X \Rightarrow W_k \subseteq X \Rightarrow W_k = X$. □

Satz 1.2.24: Sei $B \leq H \leq G$. Dann is H eine Standardparabolische Untergruppe, d.h. $\exists \nu \vDash n, H = P_\nu$

Beweis. Sei X ein H-invarianter Unterraum von V. Dann ist X auch B-invariant, wil $B \subseteq H$. Also gibt es ein $1 \leq i \leq n : X = W_i =< e_1, \ldots e_i >, \xi = (e_1, \ldots e_n)$ natürliche Basis wegen 2.2.5.
Seien $W_{\alpha_1}, \ldots, W_{\alpha_r}$ mit $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_r = n$ genau die H-invarianten Unterräume von V. $\underline{\alpha} = (\alpha_1, \ldots, \alpha_r), W_{\alpha_i} =< e_1, \ldots, e_{\alpha_i} > F_{\underline{\alpha}} = (W_{\alpha_1}, \ldots, W_{\alpha_r})$ ist H-invariante Fahne von Dimensionstyp $\underline{\alpha}$.
Sei $\mu_1 = \alpha_{1,2} = \alpha_2 - \alpha_1, \ldots, \mu_r = \alpha_r - \alpha_{r-1} \Rightarrow \mu = (\mu_1, \ldots, \mu_r) \vDash n$.
$\mathrm{Stab}_G(F_{\underline{\alpha}}) = P_\mu, H \leq P_\mu$
Zu zeigen: $H = P_\mu$.
Spezialfälle

1.) $r = 1, \mu = (n), P_\mu = G$
Zu zeigen: $H = G$
$< He_1 >= H$-invarianter Unterraum $\Rightarrow V =< He_1 > \Rightarrow \exists h \in H : he_1 = \alpha_1 e_1 + \ldots + \alpha_n e_n$ mit $\alpha_n \neq 0$
Bruhat-Zerlegung: $h \in BwB, \exists w \in W$
2.1.9 und 2.1.5 $\Rightarrow$ Für $g \in BwB$ hat g als Matrix die Form ...
d.h. hier für $h \in BwB : w(1) = n$
Beachte: Wegen $B \subseteq H$ ist $h = b_1 w b_2 \Rightarrow w = b_1^{-1} h b_2^{-1} \in H$
Sei $1 < j \leq n$ mit $w(j) = 1$ (Ohne Einschränkung $n \geq 2$)
Dann ist $X_{1j} = \{x_{1j}(\alpha) | \alpha in F\} \leq B \leq H$
$X_{n1} = X_{w(1)w(j)} = wX_{1j}w^{-1} \in H$ (mit 2.1.4)
Sei $1 \leq i < m < n \Rightarrow X_{im} \subseteq B \subseteq H$
Dann ist $X_{nm}(\alpha) = [x_{n1}(\alpha), x_{1m}(1)] \in H \forall \alpha \in F$ (mit 2.1.4)
$\Rightarrow X_{nm} \subseteq H$
$\forall 1 \leq< n : x_{i1}(\alpha) = [x_{in}(\alpha, x_{n1}(1)] \in H \Rightarrow X_{i1} \subseteq H$

$\forall 1 < i, m \leq n, i \neq m : x_{im}(\alpha) = [x_{i1}(\alpha), x_{1m}(1)] \in H \Rightarrow X_{im} \subseteq H$
Wir haben gezeigt $X_{ij} \subseteq H \forall 1 \leq i, j \leq n, i \neq j$
Da $T \subseteq B \subseteq H \Rightarrow H = G$.

2.) $r = 2, I_{\underline{\alpha}} = W_m \lneq V = W_n$
Wir wissen schon: $H \leq P_\mu, \mu = (m, n-m) \vDash n$
Klar: $U_\mu \subseteq B \subseteq H, P_\mu = U_\mu \rtimes L_\mu$, es genügt also zu zeigen: $L_\mu \subseteq H$.
$L \cong \mathrm{GL}_m(F) \times \mathrm{GL}_{n-}(F)$
$\mathrm{GL}_m(F) =<$ Diagonalmatrizen in $\mathrm{GL}_m(F)$ und $x_{ij}(\alpha) >$, analog GL_{n-m}
Es genügt also zu zeigen: $X_{ij} \in H \forall 1 \leq i, j \leq m, i$ und $m+1 \leq i, j \leq n$
Sei $X_1 =< He_1 >= H$-invarianter Unterraum von $W_m \Rightarrow X_1 = W_m$
D.h $\exists h \in H, he_1 = \alpha e_1 + \ldots \alpha_m e_m$ mit $\alpha_m \neq 0$.
Sei $w \in W$ mit $h \in BWB$. Wie oben folgt aus 2.1.9 und 2.1.5 $w(1) = m$ und daher $X_{m1} \subseteq H$.
Beachte: $w \in H \Rightarrow w^{-1}(1) = j \leq m$
$X_{m1} = X_{w(1)w(j)} = wX_{1j}w^{-1} \in H$.
Kommutatoren wie im ersten Spezialfall $\Rightarrow X_{ij} \subseteq H \forall 1 \leq i, j \leq m \Rightarrow \mathrm{GL}_m(F) \subseteq H$.
$< Hem + 1 >$ ebenfalls H-invariant $\Rightarrow \exists h \in H : he_{m+1} = \alpha_{m+1}e_{m+1} + \ldots + \alpha_n e_n$ mit $\alpha_n \neq 0$.
Es folgt analog wie eben $X_{ij} \subseteq H \forall m+1 \leq i, j \leq n \Rightarrow \mathrm{GL}_{n-m}(F) \subseteq H$.
$\Rightarrow P_\mu \subseteq H \Rightarrow H = P_\mu$

Übung: Allgemeiner Fall. □

III. Die spezielle und projektive lineare Gruppen

<u>Ziel:</u> $\mathrm{PSL}_n(F)$ ist einfach, falls $n > 2$ oder $n = 2$ und $F \neq \mathrm{GF}(2)$ oder $\mathrm{GF}(3)$ ist.

2.3.1 Erinnerung: $\det : \mathrm{GL}_n(F) - > F^* : g \mapsto \det g$ ist Gruppenhomomorphismus mit Kern $\mathrm{SL}_n(F) \trianglelefteq G, \mathrm{SL}_n(f) = \{g \in \mathrm{GL}_n(F) \mid \det g = 1\}$.
<u>Klar:</u> det ist surjektiv
Isosätze: $q - 1 = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{SL}_n(q)|} \Rightarrow |SL_n(q)| = \prod\limits_{k=1}^{n} \frac{q^k - q^{k-1}}{q-1} = \prod\limits_{k=1}^{n-1} \frac{q^k + 1 - q^k) = q^{\frac{n(n+1)}{2}} (q^n - 1)(q^{n-1} - 1}{)} \dots (q^2 - 1)$

2.3.2 Satz: $\mathrm{SL}_n(F)$ wird von den Wurzeluntergruppen (d.h. von den Transvektionen) in G erzeugt.
Beweis: Für $1 \leq i, j \leq n, i \neq j$, und f+r $\alpha \in F$ ist $x_{ij}(\alpha) \in \mathrm{SL}_n(F)$ nach 2.1.4.
In 2.1.5 haben wir gezeigt: Ist $g = (\alpha_{ij}) \in \mathrm{SL}_n(F) \subseteq G$, so gibt es ein $u \in U$ (Produkt von Transvektionen) so, dsas gilt: Für $1 \leq i \leq n$ gibt es eine eindeutig bestimmte Zeile k_i in ug so, dass der i-te Eintrag in dieser Zeile der erste von 0 verschiedene ist. Die Abbildung $\pi : i \mapsto k_i$ ist Element von $\sigma_n = W$.
Wir können diese Zeilen nach 2.1.11 durch ein Produkt $\tilde{\pi}$ von Transvektionen $\widetilde{(i,j)} = x_{ij}(1)x_{ji}(-1)x_{ij}(1)$ ($(i,j) \in \sigma_n$ Transposition) bis aufs Vorzeichen ordnen. ($\widetilde{(i,j)} = diag(1, \dots, 1, -1, 1, \dots$ (i,j)). Daraus folgt: durch ein Produkt $b \in \mathrm{SL}_n(F)$ von Transvektionen wird $b \cdot g$ eine obere Dreiecksmatrix $\tilde{g}$.
Also $bg = \tilde{g} = \begin{pmatrix} \lambda_1 & & A \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$. Beachte: $\det \tilde{g} = \det b \cdot \det g = 1$, d.h. $\tilde{g} \in \mathrm{SL}_n(F)$.
$\Rightarrow \det \tilde{g} = \lambda_1 \cdot \ldots \cdot \lambda_n = 1$.

Beachte: Seien $\alpha, \beta, \gamma \in F$ mit $\alpha\gamma \neq 0$.
$x_{21}(-1)x_{12}(1 - \gamma^{-1})x_{21}(y) \cdot \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 - \gamma^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$
$= \begin{pmatrix} 1 & 1 - \gamma^{-1} \\ -1 & \gamma^{-1} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \alpha\gamma & \gamma\beta + \gamma \end{pmatrix} = \begin{pmatrix} \alpha + \alpha\gamma - \alpha & \beta + \gamma\beta + \gamma - \beta - 1 \\ -\alpha + \alpha & -\beta + \beta + 1 \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \gamma\beta - \beta - 1 \\ 0 & 1 \end{pmatrix}$

Auf alle Zeilen von $\tilde{g}$ anwenden.

$\Rightarrow$ Man kann $\tilde{g}$ durch Premultiplikation mit einem Produkt von Transvektionen auf die Gestalt $\tilde{g}' = \begin{pmatrix} \lambda_1 \cdot \ldots \cdot \lambda_n & & * \\ & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in U$ bringen. Jedes Element von U ist aber Produkt von Transvektionen (elementare Zeilenoperationen: $\tilde{g}' \rightsquigarrow 1$). Also ist $\tilde{g}'$ Produkt von Transvektionen. Also ist g Produkt von Transvektionen.

2.3.3 Satz: Die Wurzeluntergruppen $X_{ij}, 1 \leq i, j \leq n, i \neq j$, sind in $\mathrm{SL}_n(F)$ konjugiert.
Beweis: Seien $1 \leq i, j \leq n, 1 \leq k, l \leq n, i \neq j, k \neq l$.
σ_n ist n-fach transitiv auf $\{1, \ldots, n\}$, also zweifach transitiv $\Rightarrow \exists w \in W = \sigma_n : w(i) = k, w(j) = l$.
Haben gesehen: $wX_{ij}w^{-1} = X_{w(i),w(j)} = X_{kl}$. Ist w gerade Permutation, d.h. $\operatorname{sign} w = \det w = 1 \Rightarrow w \in \mathrm{SL}_n(F)$ und wir sind fertig.

Sei also $\operatorname{sign} w = \det w = -1$ und $\alpha in F$. Sei $d = d^{-1} = \begin{pmatrix} -1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in \mathrm{GL}_n(F)$. Dann ist $\det(dw) = \det d \cdot \det w = -\det w = 1$, d.h. $dw \in \mathrm{SL}_n(F)$.
$dwX_{ij}(dw)^{-1} = d(wX_{ij}w^{-1})d = dX_{kl}d = d(E+\alpha e_{kl})d = dEd+\alpha de_{kl}d = \begin{cases} X_{kl}(\alpha) & \text{für } k, l \neq 1 \\ X_{kl}(-\alpha) & \text{sonst, } (k \neq l) \end{cases}$
In jedem Fall ist $(dw)X_{ij}(dw)^{-1} = X_{kl}$.

Definition: Sei $Z = \{\alpha E \mid \alpha \in F^*\}, E = 1$. Dann ist $Z \leq G, G \subseteq Z(G) =$ Zentrum von G.
2.3.4 Satz: $Z = Z(G)$ und $Z \cap \mathrm{SL}_n(F) = Z(\mathrm{SL}_n(F))$.
Es genügt zu zeigen: Jedes Element von $\mathrm{GL}_n(F)$ (bew. $\mathrm{SL}_N(F)$), das mit allen Transvektionen $x_{ij}(1)$ $(1 \leq i, j \leq n, i \neq j)$ vertauscht, liegt schon in Z.
Sei $g = (\alpha_{ij}) = \sum_{i,j} \alpha_{ij}e_{ij} \in Z(G) \Rightarrow g \cdot x_{rs}(1) = x_{rs}(1) \cdot g \forall 1 \leq r, s \leq n, r \neq s \Leftrightarrow g(E+e_{rs}) = (E + e_{rs})g \Leftrightarrow \sum_{ij} \alpha_{ij}e_{ij}e_{rs} = \sum_{kl} \alpha_{kl}e_{rs}e_{kl} \Leftrightarrow \sigma_i\alpha_{ir}e_{is} = \sum_l \alpha_{sl}e_{rl}$
d.h. $e_{is} = e_{rl} \Leftrightarrow i = r, l = s, \alpha_{rr} = \alpha_{ss}, r \neq s, \alpha_{ij} = 0$ sonst.
$\Rightarrow g = \alpha \cdot E \in Z$. (Für $\mathrm{SL}_n(F) : \alpha^n = \det \alpha E = 1$)

Definition: $\mathrm{GL}_n(F)/Z = \mathrm{PGL}_n(F) =$ „projektive allgemeine lineare Gruppe“
$\mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F)) = \mathrm{PSL}_n(F) =$ „projektive spezielle lineare Gruppe“

2. Isosatz: $\mathrm{PSL}_n(F) \cong \mathrm{SL}_n(F)/(Z \cap \mathrm{SL}_n(F)) = Z \cdot \mathrm{SL}_n(F)/Z \leq \mathrm{GL}_n(F)/Z = \mathrm{PGL}_n(F)$
Für $F = \mathrm{GF}(q) = (F)_q : |\mathrm{PGL}_n(q)| = \frac{\mathrm{GL}_n(q)}{Z} = \frac{\mathrm{GL}_n(q)}{q-1} = |\mathrm{SL}_n(q)|$

Bemerkung:

1) $\mathrm{GL}_n(F) = \mathrm{SL}_n(F) \rtimes \left\{ \begin{pmatrix} \alpha & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \mid \alpha \in F^* \right\}$

2) F algebraisch abgeschlossen $\Rightarrow$ $z := (\sqrt[n]{\det g}^{-1} E) \in Z, g \cdot z \in \mathrm{SL}_n(F)$, es folgt: $\mathrm{PSL}_n(F) \cong \mathrm{PGL}_n(F)$.

3) $\mathrm{PSL}_2(2) \cong \sigma_3 \trianglerighteq A_3$, da $\mathrm{PSL}_2(2) \cong GL_2(2)$
$\mathrm{PSL}_2(3) \cong A_4 \trianglerighteq V_4 \cong G_2 \times G_2$

2.3.6 Lemma: Sei $n \geq 2$; und $|F| \neq 2, 3$ für $n = 2$. Dann ist jede Tranvektion $x_{ij}(\alpha)$ $(1 \leq i, j \leq n, i \neq j, \alpha \in F)$ ein Kommutator von Elementen in $\mathrm{SL}_n(f)$.
Beweis: Ist $n > 2$, dann ist $x_{ij}(\alpha) = [x_{ij}(\alpha), x_{kj}(\alpha)]$ mit $1 \leq k \leq n, k \neq i, k \neq j$.
Sei $n = 2, \beta, \gamma \in F$ mit $\beta \neq 0$.
$[\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}] = \begin{pmatrix} 1 & (\beta^2 - 1)\gamma \\ 0 & 1 \end{pmatrix}$
$\Rightarrow x_{12}(\alpha)$ ist Kommutator dieser Elemente aus $\mathrm{SL}_2(F)$, falls es $\beta, \gamma \in F$ mit $\beta \neq 0$ gibt, so dass $\alpha = (\beta^2 - 1)\gamma$ ist.
Sei $|F| > 3$, dann gibt es immer ein $\beta \in F^*$ mit $\beta^2 \neq 1$ und $\gamma = \alpha(\beta^2 - 1)^{-1}$.
$x_{21}(\alpha)$ ähnlich bzw. ist konjugiert in $\mathrm{SL}_2(F)$ zu einem Element aus X_{12}.

2.3.7 Korrolar: Sei $n > 2$ oder $|F| > 3$ für $n = 2$. Dann ist $\mathrm{SL}_n(F) = [\mathrm{SL}_n(F), \mathrm{SL}_n(F)]$.

2.3.8 Lemma: Sei $n \leq 2$ $\mathrm{SL}_n(F)$ operiert auf der $\{Fv | 0 \neq v \in F^n\}$ durch $g(Fv) := F(gv)$ (Kern ist das Zentrum).
Diese Operation ist 2-fach transitiv.
Beweis: Seien $c_1, c_2, d_1, d_2 \in F^n \setminus \{0\}$ und c_1, c_2 bzw. d_1, d_2 linear unabhängig, d.h. $Fc_1 \neq Fc_2, Fd_1 \neq Fd_2$.
Ergänze c_1, c_2 bzw. d_1, d_2 zu Basen $\tilde{C} = (c_1, c_2, \ldots, c_n)$ und $\tilde{D} = (d_1, d_2, \ldots, d_n)$ von F^n. Sei $C = m_{\mathrm{id}}(\xi, \tilde{C}) = m_f(\xi, \xi)$ mit $f(e_i) = c_i$.
$D = m_{\mathrm{id}}(\xi, \tilde{D}) = m_g(\xi, \xi)$ mit $g(e_i) = d_i$
Dann sind $C, D \in \mathrm{GL}_n(F)$. Sei $\epsilon = \det D / \det C = \det(DC^{-1}), A = \begin{pmatrix} \epsilon & 0 \\ 0 & 1_{n-1} \end{pmatrix}, \det A = \epsilon, B = DA^{-1}C^{-1}$, so ist $Bc_1 = \epsilon^{-1} d_1, Bc_i = d_i$ für $i > 2$ x
$BFc_i = FBc_i = Fd_i$ für alle i. Klar: $\det B = 1$, d.h. $B \in \mathrm{SL}_n(F)$ $\square$.

Missing: 27.11.2009
$|G| = p^a m, p \nmid m, |G|_p = p^a, |G|_{p'} = m$

$\mathrm{Syl}_p(G) \equiv 1 \mod p$ Beweis: $X = \{A \subseteq G \mid |A| = |G|_p = p^a\}$ G-Menge
Bemerkung: $P \in \mathrm{Syl}_p(G) \Rightarrow P \in X$
$A \in X$ so gibt es ein $g \in G : g \cdot A \ni 1$

$|X| = \binom{p^a \cdot m}{p^a} = \sum_{O \in G\text{-Bahnen von } X} |O|$
Sei $A \in X, A \in O =$ Orbit von Xso, dass $1 \in A$. Sei $P = \mathrm{Stab}_G(A) \leq G$. Dann ist $P \subseteq P \cdot A = A \Rightarrow |P| \leq |A| = p^a$
$1.3.7 \Rightarrow |O| = |G : P|$.
Angenommen p teilt nicht $|G : P|$, so ist $|G|_p$ Teiler von $|P|$. Also ist $|G|_p = |P| = p^a$ und $P \in \mathrm{Syl}_p(G)$ und $|O| = m$.
Sei umgekehrt $P \in \mathrm{Syl}_p(G)$. Dann ist die G-Menge $G/P = \cup g_i P$ mit $|g_i P| = |P| = p^a$, d.h. G/P ist ein Orbit O in X: $|O| = |G : P| = m$
Klar: $\mathrm{Stab}_G(1 \cdot P) = P$
Auf diese Weise erhalten wir eine Bijektion zwischen der Menge der G-Bahnen in $X' := \{A \in X \mid p \nmid |G \cdot A|\}$
Also ist $X' =$ Vereinigung aller Bahnen O von X mit $p \nmid |O|$
$X \backslash X' =$ Vereinigung aller Bahnen O von X mit $p \mid |0|$ und daher $p \mid |X \backslash X'| = |X| - |X'|$
Also $|X| \equiv |X'| \mod p$
Sei $r = |\mathrm{Syl}_p(G)| =$ Anzahl der p-Sylow Untergruppen von $G = |\{$Bahnen O von X mit $O \subseteq X'\}|$.
Es gilt dann: $r \cdot m = |X'| \equiv_p |X| \equiv_p \binom{p^a m}{p^a}$
$p \nmid m \Rightarrow r \mod p$ ist nur von $|G|$ und nicht von G selbst abhängig. Das heißt je zwei Gruppen G und H mit $|G| = |H|$ haben $\mod p$ dieselbe Anzahl von p-Sylowgruppen.
Sei $G = C_{p^a m}$, dann ist $r \equiv 1 \mod p$, also ist $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$ für alle G mit $G = p^a m$.
Insbesondere ist $r \neq 0$, d.h. G besitzt mindestens eine p-Sylow Untergruppe.
Dies zeigt 1) und 4).

Sei nun $P \in \mathrm{Syl}_p(G), G$ Gruppe der Ordnung $p^a m, p^a = |G|_p, Q \leq G$ p-Gruppe.
$Y = \{gPg^{-1} \mid g \in G\}$. Q operiert auf Y durch Konjugation:
${}^x(yPy^{-1}) = xyP(xy)^{-1} \in Y$ für $x \in X$.

Sei O ein Q-Orbit von Y, $P_1 \in O$. Dann ist $|O| = |Q : \mathrm{Stab}_Q(P_1)| =$ Potenz von p (möglicherweise p^0).
Aber $|Y| = |G : N_G(P)|$ Teiler von m (1.3.15) $\Rightarrow p \nmid |Y|$.Also muss es eine Q-Bahn O in Y geben mit $p \nmid |O| \Rightarrow \exists Q$-Bahn O in Y mit $|O| = p^0 = 1 \Rightarrow O = \{P_1\}$. Dann ist also $xP_1x^{-1} = P_1 \forall x \in Q$. Daher ist $QP_1 = P_1 Q$ und mit (1.1.4) ist $QP_1 \leq G$
Klar ist: $|P_1| \leq |QP_1|$. Nach 1.3.12 ist $|QP_1| = \frac{|Q||P_1|}{|Q \cap p_1|} = |P_1||Q : Q \cap P_1|$. Also ist QP_1 eine p-Untergruppe von G.
Also ist wegen $|P_1| \leq |QP_1|$ die Ordnung $|Q \cdot P_1|$ von QP_1 gleich $P_1 = p^a$ und daher $|Q \cap P_1| = |Q| \Rightarrow Q \subseteq P_1 \in \mathrm{Syl}_p(G)$. Dies zeigt 3).

Seien $Q, P \in \mathrm{Syl}_p(G) \Rightarrow$ (nach vorigem Schritt) $\exists g \in G : Q \leq gPg^{-1}$. Wegen $|Q| = |P| = p^a$ ist $Q = gPg^{-1}$. □

2. Beweis für Existenz von p-Sylowuntergruppen:

Induktion über $|G|$
$|G| = 1$ trivial
$p \nmid |G|$ trivial
$|G| = p^a m$ mit $p \nmid m > 1$, und sei die Behauptung beweisen für alle Gruppen $|H|$ mit $|H| < |G|$.
Besitzt G eie echte Untergruppe H mit $p \nmid [G : H]$, so ist jede p-Sylowgruppe von H eine p-Sylowgruppe von G und wir sind fertig.
Ohne Einschränkung gelte $H \lneqq G \Rightarrow p \mid [G : H]$
Klassengleichung 1.3.13:
$|G| = |Z(G)| + \sum\limits_{i=1}^{l} [G : C_G(g_i)]$ mit $\{g_1, \dots, g_l\}$ Repräsentanten von Konjugationsklassen von G der Größe > 1.
Für $1 \leq i \leq l$ ist $C_G(g_i) \lneqq G$ und daher $p \mid [G : C_G(g_i)]$
Also teilt $p \mid Z(G) =$ abelsche Gruppe. Also ist $|Z(G)| > 1$.
$\Rightarrow G$ besitzt eine normale Untergruppe N ($\leq Z(G)$) der Ordnung p. $|G/N| = p^{a-1}m < p^a m \Rightarrow \exists \overline{P} \in \mathrm{Syl}_p(G/N)$
Sei $P =$ volles Urbild von $\overline{P}$ in $G \Rightarrow N \trianglelefteq P, P/N = \overline{P} \Rightarrow |P| = p^a \Rightarrow P \in \mathrm{Syl}_p(G)$.

Korrolar: Sei $|G| = p^a m, p^a = |G|_p$. Dann gibt es für $1 \leq b \leq a$ eine Untergruppe H von G mit $|H| = p^b$ (Weil $P \in \mathrm{Syl}_p(G)$ eine p-Gruppe, daher nilpotent und damit auflösbar ist. Wir können $H \leq P$ wählen!).

3.1.3 Korrolar: $|\mathrm{Syl}_p(G)|$ ist Teiler von $|G|_{p'} = \frac{|G|}{|G|_p}$ $(|G| = p^a m, p \nmid m)$
Beweis: G operiert auf $\mathrm{Syl}_p(G)$ per Konjugation transitiv. Also ist $P \in \mathrm{Syl}_p(G)$, so ist $|\mathrm{Syl}_p(G)| = [G : \mathrm{Stab}_G(P)]$. Wegen $P \trianglelefteq N_G(P) \leq G$ ist daher $|\mathrm{Syl}_p(G)|$ Teiler von m.

3.1.4 Korrolar: (Cauchy's Theorem) G hat ein Element der Ordnung p $(p \mid |G|)$
3.1.5 Satz: Sei $N \trianglelefteq G (N \neq G)$, und sei $P \in \mathrm{Syl}_p(G)$. Dann ist $PN/N \in \mathrm{Syl}_p(G/N)$ und $P \cap N \in \mathrm{Syl}_p(N)$.
Beweis: $[G/N : PN/N] = [G : PN]$ wegen 3. Isosatz. $PN/N \cong P/(P \cup N) \Rightarrow PN/N$ ist Gruppe.
$p \nmid [G : P] = |G|_{p'} \Rightarrow [G : PN]$ ist Teiler von m, wird nicht von p geteilt.
$\Rightarrow PN/N \in \mathrm{Syl}_p(G/N)$.
Nach 1.3.12 ist $[PN : P] = \frac{|P| \cdot |N|}{|P \cap N||P|} = \frac{|N|}{|P \cap N|} \Rightarrow$ (nach oben) $P \cap N$ ist p-Untergruppe von N mit $[N : P \cap N]$ wird nicht von p geteilt. Also ist $P \cap N \in \mathrm{Syl}_p(N)$. $\square$
Vorsicht: $H \leq G \not\Rightarrow H \cap P \in \mathrm{Syl}_p(H)$ für $P \in \mathrm{Syl}_p(G)$

3.1.6 Satz: Sei $H \leq G, P \in \mathrm{Syl}_p(G)$. Dann gibt es $g \in G$ so, dass $gPg^{-1} \cap H \in \mathrm{Syl}_p(H)$ ist.
Beweis: Sei $Q \in \mathrm{Syl}_p(H) \Rightarrow \exists P' \in \mathrm{Syl}_p(G)$ mit $Q \subseteq P' \Rightarrow \exists g \in G$ mit $P' = gPg^{-1} \cap H \supseteq Q$
Klar: $Q = P' \cap H$ (warum?)

Anwendungen:

3.1.7 Satz („pq-Theorem“): Seien p, q Primzahlen mit $p > q$. Sei G Gruppe mit $|G| = p \cdot q$. Dann ist G abelsch (und daher $\cong C_{q \cdot p} \cong C_q \times C_p$) oder $p \equiv 1 \mod q$. Ist dies so, dann gibt es bis auf Isomorphie genau eine nicht abelsche Gruppe der Ordnung $p \cdot q$.
Beweis: Sei $P \in \mathrm{Syl}_p(G), Q \in \mathrm{Syl}_q(G) \Rightarrow |P| = p, |Q| = q \Rightarrow P \cong C_p \wedge Q \cong C_q$. Wir haben $P \cap Q = (1)$, und daher ist $G = P \cdot Q$ (1.3.12). Mit 3.1.3 folgt $|\mathrm{Syl}_p(G)| \mid [G : P]$ und mit 3.1.4 $|\mathrm{Syl}_p(G)| \cong 1 \mod p$
$\Rightarrow |\mathrm{Syl}_p(G)| = 1 = [G : N_G(P)] \Rightarrow N_G(P) = G \Rightarrow P \trianglelefteq G$ ($p > q \Rightarrow q \not\cong 1 \mod p$).

Ist $p \not\cong 1 \mod q \Rightarrow$ (analog) $Q \trianglelefteq G \Rightarrow G = P \times Q$

Sei also $p \cong 1 \mod q$. Sei G nicht abelsch, $\varphi : Q \to \mathrm{Aut}(P) : x \mapsto c_x, c_x : P \to P : y \mapsto xyx^{-1}$.
$\ker \varphi \neq (1) \Rightarrow \ker \varphi = Q \Rightarrow \varphi Q \Rightarrow (1) \leq P$ und $c_x = \mathrm{id}_P \Rightarrow G = P \times Q$, G abelsch. Widerspruch!
Also ist $\ker \varphi = (1)$, d.h. φ ist injektiv. Sei $P =< g >$. Leicht: Sei $1 \leq i \leq p-1$, so induziert $g \mapsto g^i$ einen Automorphismus σ_i von $P = C_p =< g >$, und $\mathrm{Aut}(P) = \{\sigma_i | 1 \leq i \leq p-1\}$ ist zyklisch der Ordnung $p-1$.

Nun ist $q \mid p-1$, also hat $C_{p-1} \cong \mathrm{Aut}(C_p)$ eine eindeutige Untergruppe der Ordnung q, und diese ist isomorph zu $C_q \cong Q$.
Also: Unter φ wird Q auf die eindeutig bestimmte Untergruppe der Ordnung q von $\mathrm{Aut}(P)$ abgebildet.
Beachte: Ist $\psi : Q \to \mathrm{Aut}(P)$ ein Monomorphismus, so ist $\mathrm{im}\,\varphi = \mathrm{im}\,\psi$, es gibt aber viele Monomorphismen von $Q \to \mathrm{Aut}(P)$.
Für jeden solchen Monomorphismus ψ haben wir eine Gruppe $P \rtimes_\psi Q$.
Der nächste Satz zeigt: Alle diesen semidirekten Produkte sind isomorph. Also gibt es in diesem Fall ($p \cong 1 \mod q$) genau eine nichtabelsche Gruppe der Ordnung $p \cdot q$. □

3.1.8 Satz: Sei H zyklische Gruppe, N Gruppe. Seien φ, ψ Monomorphismen von $H \to \mathrm{Aut}(N)$ mit $\mathrm{im}\,\varphi = \mathrm{im}\,\psi$. Dann ist $N \rtimes_\varphi H \cong N \rtimes_\psi H$.
Beweis: Sei $H =< x >$. Wegen $\varphi(H) = \psi(H)$ ist $< \varphi(x) >=< \psi(x) >\leq \mathrm{Aut}(N)$. Es gibt also $a, b \in \mathbb{Z}$ mit $\varphi(x)^a = \psi(x)$ und $\psi(x)^b = \varphi(x)$. Für $s \in \mathbb{Z}$ ist dann $\varphi((x^s)^a) = \varphi(x)^{as} = \psi(x)^s = \psi(x^s)$, d.h. $\varphi(h^a) = \psi(h) \forall h \in H$, analog $\psi(h^b) = \varphi(h) \forall h \in H$.
Definiere $\tau : N \rtimes_\psi H \to N \rtimes_\varphi H$ durch $\tau(n \cdot h) = n \cdot h^a$ und $\lambda : N \rtimes_\varphi H \to N \rtimes_\psi H$ durch $\lambda(n \cdot h) = n \cdot h^b$
$\tau(n_1 h_1 n_2 h_2) = \tau(n_1 \psi(h_1)(n_2) h_1 h_2) = n_1 \psi(h_1)(n_2)(h_1 h_2)^a = n_1 \varphi(h_1^a)(n_2) h_1^a h_2^a = n_1 h_1^a n_2 h_2^a = \tau(n_1 h_1) \tau(n_2 h_2)$
$\Rightarrow \tau$ (und analog λ) ist Gruppenhomomorphismus.
Nun ist $\tau\lambda : nh \mapsto \tau(n \cdot h^b) = n \cdot h^{ba}$, aber $\varphi(x) = \psi(x)^b = (\varphi(x^a))^b = \varphi(x^{ab})$ und φ ist injektiv. Also ist $x = x^{ab}$ und daher $h = h^{ab} \forall h \in H$, also ist $\tau\lambda = \mathrm{id}_{N \rtimes_\varphi H}, \lambda\tau = \mathrm{id}_{N \rtimes_\psi H}$
Also sind τ, λ Isomorphismen und $N \rtimes_\varphi H \cong N \rtimes_\psi H$, □.

Erinnerung: A_5 ist einfach $A_5 \leq \sigma_5$, $|\sigma_5| = 5! = 120 \Rightarrow A_5 = 60 = 3 \cdot 5 \cdot 2^2$.

3.1.9 Satz: Sei G einfach, $|G| = 60$. Dann ist $G \cong A_5$.
Beweis: Sei $n \in \mathbb{N}$ und $H \lneq G$ mit $[G : H] = n$. Sei $\rho : G \to \sigma_n$ die Darstellung, die zu der G-Menge G/H gehört. $\Rightarrow \rho$ ist injektiv. Insbesondere ist $|G| = 60 \leq n! \Rightarrow n \geq 5$.
Beh: G besitzt eine Untergruppe von H mit $[G : H] = 5$.
Angenommen, G besitzt keine solche Untergruppe: $|\mathrm{Syl}_2(G)| \neq 1$ teilt $3 \cdot 5 = 15$, sonst wäre G nicht einfach. Sei $P \in \mathrm{Syl}_2(G)$. Betrachte Möglichkeiten für $|\mathrm{Syl}_2(G)|$:
3: $[G : N_G(P)] = 3 < 5$ Widerspruch!
5: $[G : N_G(P)] = 5$ Widerspruch zur Annahme
Also ist $[G : N_G(P)] = 15$ Seien $S_1, S_2 \in \mathrm{Syl}_2(G), S_1 \neq S_2$. Sei $1 \neq t \in S_1 \cap S_2$. $V_4 = C_2 \times C_2, C_4$ sind die einzigen Gruppen der Ordnung 4. $\Rightarrow S_1$ und S_2 sind abelsch $\Rightarrow |C_G(t)| > 4$ und $4 \mid |C_G(t)|$, da $S_1 \leq C_G(t)$. $\Rightarrow [G : C_G(t)] \in \{1, 3, 5\} \Rightarrow [C : C_G(t)] = 1 \Rightarrow t \in Z(G) \trianglelefteq G$ Widerspruch zur Einfachheit von G.
Also hat $G : 15(4 - 1) = 45$ der Ordnung 2 oder 4. Da G einfach ist, gilt für $P \in \mathrm{Syl}_5(G)$: $1 \neq [G : N_G(P)] \mid 4 \cdot 3$ und $[G : N_G(P)] \cong 1 \mod 5$, also nicht $\{1, 2, 3, 4, 12\}$ - also hat G genau 6 5-Sylowgruppen, und daher $6(5 - 1) = 24$ Elemente der Ordnung 5. Also ist $|G| \leq 45 + 24 > 60$ Widerspruch. Also hat G eine Untergruppe H mit $[G : H] = 5$.
Sei wieder $\varphi : G \to \sigma_5$ die Darstellung auf G/H. Diese ist injektiv, so ist G ohne Einschränkung Untergruppe von σ_5 vom Index 2, da die $|G| = 60 = \frac{120}{2} = \frac{|\sigma_5|}{2}$. Also ist $G \trianglelefteq \sigma_5$. Angenommen $G \neq A_5 \Rightarrow |G \cdot A_5| > 60 \Rightarrow G \cdot A_5 = \sigma_5$.
Nach 1.3.12: $|G \cap A_5| = \frac{|G||A_5|}{G \cdot A_5} = 30$. Also ist $G \cap A_5$ Untergruppe von G vom Index 2 - Widerspruch. Also $G = A_5$.

3.1.10 Korrolar: $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$, da $\mathrm{PSL}_2(4)$ und $\mathrm{PSL}_2(5)$ einfach mit Ordnung 60.

Bemerkung: Man kann zeigen: Alle anderen Gruppen $\mathrm{PSL}_n(q)$ sind paarweise verschieden (?).
Relativ leichte Übung: Ist G einfach und $|G| < 60$ so folgt $G \cong C_{|G|}$

3.1.11 Satz „Frattini Argument“: Sei G endliche Gruppe, $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(N)$, p Primzahl. Dann ist $G = N_G(P) \cdot N$.
Beweis: Sei $g \in G$. Wegen $gNg^{-1} = N \trianglelefteq G$ ist $gPg-1 \subseteq N \Rightarrow gPg^{-1} \in \mathrm{Syl}_p)N)$. Also gibt es $n \in N : n(gPg^{-1})n^{-1} = P = ngP(ng)^{-1} \Rightarrow ng \in N_G(P) \Rightarrow g \in n^{-1}N_G(P) \subseteq NN_G(P) = N_G(P)N$. $\square$

IV. Normalteilerstruktur

1. Satz von Jordan-Hölder

Sei im folgenden G eine beliebige Gruppe.

4.1.1 Definition: Sei Ω eine Menge, dann heißt G Gruppe mit Operatorenbereich Ω (kurz Ω-Gruppe), falls es eine externe binäre Verknüpfung $\Omega \times G \to G : (\alpha, g) \mapsto \alpha g \in G$ gibt mit $\alpha(g_1 g_2) = (\alpha g_1)(\alpha g_2) \forall g_1, g_2 \in G, \alpha \in \Omega$.
Äquivalente Formulierung: Es gibt eine Abbildung von $\Omega \to \{\sigma : G \to G \mid \sigma \text{ ist Gruppenhom.}\}$.

Eine Untergruppe H der Ω-Gruppe G heißt zulässig (Ω-Untergruppe, $H \leq_\Omega G$), falls $\alpha h \in H \forall h \in H, \alpha \in \Omega$, und sie heißt zulässiger Normalteiler (Ω-Normalteiler, $H \trianglelefteq_\Omega G$), wenn H zusätzlich Normalteiler von G ist.

Klar: Homomorphismen von Ω-Gruppen: $F : G \to X$ Gruppenhomomorphismus mit $f(\alpha g) = \alpha f(g)$, G, X Ω-Gruppen, $g \in G, \alpha \in \Omega$
Es gelten Isosätze, Kerne von Ω-Homomorphismen sind Ω-Normalteiler, Bilder sind Ω-Untergruppen.
Eine Ω-Gruppe heißt einfach, falls sie keine nichttrivialen Ω-Normalteiler hat.

4.1.2 Beispiele: G : Ω-Gruppe

i) $\Omega = \emptyset$: zulässigen Untergruppen = Untergruppe von G, zulässigen Normalteiler = Normalteiler von G.

ii) $\Omega = \mathrm{Inn}(G)$ ($\Omega = G$ operiert durch Konjugation auf G): zulässigen Untergruppen = zulässigen Normalteiler = Normalteiler von G.

iii) $\Omega = \mathrm{Aut}(G)$: zulässigen Untergruppen = char. Untergruppen von G.

iv) $G = (R, +)$ = add. Gruppe eines Rings R mit 1 (alle Untergruppen sind Normalteiler) $\Omega = R$ operiert auf G per Multiplikation von links (rechts). Die Ω-Untergruppen von $(R, +)$ sind genau die Linksideale (Rechtsideale) von R. Links-Rechts-Operation: $\Omega \times G \times \Omega \to G : (\alpha, g, \beta) \mapsto \alpha g \beta$ mit $(\alpha g)\beta = \alpha(g\beta)$.

Für $(R,+)$ mit $\Omega = R$ sind dann die zulässigen Untergruppen die Ideale von R.

v) $M = G =$ additive abelsche Gruppe mit R-Modul, $R = \text{Ring} \ni 1$, M ist eine R-Gruppe unter Linksmultiplikation mit Elementen von R.
Die zulässigen R-Untergruppen = zulässige R-Normalteiler = Untermoduln (analog für Rechtsmoduln).

Jetzt sei Ω eine Menge und G eine Ω-Gruppe.

Definition: Eine endliche Folge $G = G_0 >_\Omega G_1 >_\Omega G_2 >_\Omega \ldots >_\Omega G_r = (1)$ von Ω-Untergruppen heißt Kompositionsreihe von G, falls $G_{i+1} \trianglelefteq_\Omega G_i$ und G_i/G_{i+1} ist einfache Ω-Gruppe.

Beispiel: $\sigma_5 \trianglerighteq A_5 \trianglerighteq (1)$ ist eine Kompositionsreihe mit „Kompositionsfaktoren“ $\sigma_5/A_5 \cong C_2, A_5 = A_5/(1)$.

Definition: N ist maximale normale Ω-Untergruppe von G, falls $G \neq N \trianglelefteq_\Omega G$ und kein Ω-Normalteiler von G echt zwischen N und G existiert $\Rightarrow G/N$ einfache Ω-Gruppe.

Beachte: Für Ω-Gruppen gelten die 3 Isomorphiesätze, und daher der Korrespondenzsatz 1.1.11.

4.1.3 Satz: Endliche Gruppen ($\Omega = \emptyset$) besitzen Kompositionsreihen. Beweis klar.

4.1.4 Korrolar: Sei G endliche Gruppe ($\Omega = \emptyset$), und sei $N \trianglelefteq G$. Dann besitzt G eine Kompositionsreihe „durch“ N, d.h. N kommt als eine der Untergruppen G_i vor.
Beweis: Sei $N = N_0 > N_1 > N_2 > \ldots > N_k = (1)$ Kompositionsreihe von N und $G/N = H_0 > H_1 > \ldots > H_r = (1)$ Kompositionsreihe von G/N, G_i = volles Urbild von H_i in G/N, also $G_i = \{g \in G \mid gN \in H_i\}$.
1.1.11 $\Rightarrow G = G_0 > G_1 > \ldots > G_{r-1} > N = N_0 > \ldots > N_k = (1)$ Kompositionsreihe von G durch N.

4.1.5 Lemma: Sei G beliebige Ω-Gruppe mit einer Kompositionsreihe. Sei $N \trianglelefteq_\Omega G$, dann besitzt N ebenfalls eine Kompositionsreihe.
Beweis: Sei $G = G_0 > G_1 > \ldots > G_r = (1)$ Kompositionsreihe von G. Sei $N_i = N \cap G_i$. Dann ist $N = N_0 \geq N_1 \geq \ldots \geq N_r = (1)$
Dann ist $N_{i+1} = G_{i+1} \cap N \trianglelefteq N_i = G_i \cap N$ und $N_i/N_{i+1} = (N \cap G_i)/(N \cap G_{i+1}) = (N \cap G_i)/((N \cap G_i) \cap (G_{i+1})) \cong$ (2. Isosatz) $((N \cap G_i)G_{i+1})/G_{i+1} \trianglelefteq G_i/G_{i+1}$ (Korrespondenzsatz)
Also ist, da G_i/G_{i+1} einfach ist, entweder $N_i/N_{i+1} = (1)$ (d.h. $N_i = N_{i+1}$), oder $N_i/N_{i+1} \cong G_i/G_{i+1}$ einfach.
So erhalten wir eine Kompositionsreihe von N durch Streichung der Wiederholungen in $N = N_0 \geq N_1 \geq \ldots \geq N_r = (1)$. $\square$

Definition: Eine Kette $G = G_0 > G_1 > \ldots > G_r = (1)$ heißt Ω-Subnormalkette, falls $G_{i+1} \trianglelefteq_\Omega G$ ist, und Ω-Normalkette, falls $G_i \trianglelefteq_\Omega G$ ist.

Seien $G = G_0 > G_1 > \ldots > G_r = (1)$ und $G = H_0 > H_1 > \ldots > H_r = (1)$ zwei Subnormalketten derselben Länge r. Dann heißen diese äquivalent, fall es ein $\rho \in \sigma_r$ gibt mit $G_{i-1}/G_i \cong H_{\rho(i)-1}/H_{\rho(i)}$ für $1 \leq i \leq r$.
Klar: Dies ist eine Äquivalenzrelation auf der Menge der Subnormalketten der Länge r von G.

4.1.6 Satz (Jordan-Hölder): Sei G eine Ω-Gruppe und besitze G eine Kompositionsreihe. Dann haben je zwei Kompositionsreihen von G dieselbe Länge und sind äquivalent.
Konsequenz: In einer Kompositionsreihe einer Ω-Gruppe (= einfache Ω-Gruppen), sind die vorkommenden einfachen Kompositionsfaktoren mit ihren Multiplizitäten eindeutig bestimmt (aber nicht die Reihenfolge).

Beweis: Seien $G = G_0 > G_1 > \ldots > G_r = (1)$ und $G = H_0 > H_1 > \ldots > H_s = (1)$ zwei Kompositionsreihen von G.
Induktion über r:
$r = 0$: $G = (1)$ trivial.
$r = 1$: $G \trianglerighteq (1)$ ist Kompositionsreihe $\Rightarrow G$ ist einfach $\Rightarrow s = s, H_1 = (1)$.
Sei $r > 1$ und die Behauptung bewiesen für alle Ω-Gruppen mit einer Kompositionsreihe der Länge $< r$.
Ist $G_1 = H_1$, so hat $G_1 = H_1$ die Kompositionsreihe $G_1 > G_2 > \ldots > G_r = (1)$ der Länge $r-1$ und $H_1 > H_2 > \ldots > H_s = (1)$, die nach Induktionsvoraussetzung äquivalent sind und $r - 1 = s - 1$, also $r = s$ und mit $G_/G_1 = H/H_1$ fertig.
Sei also $G_1 \neq H_1$. Wegen $G_1 \trianglelefteq G_0 = G, H_1 \trianglelefteq H_0 = G$ ist $G_1 \lneq G_1H_1 \trianglelefteq G$. Da G/G_1 einfach ist, ist also $G_1H_1 = G$.
Sei $K = G_1 \cap H_1$, dann ist $G/G_1 \cong H_1/K$ und $G/H_1 \cong G_1/K$.
Also sind G_1/K und H_1/K einfache Ω-Gruppen.
Beachte $K \trianglelefteq G$, also besitzt K eine Kompositionsreihe $K = K_0 > K_1 > \ldots > K_t = (1)$.
$G_1 > K_0 > K_1 > \ldots > K_t = (1)$ ist Kompositionsreihe von G der Länge $t + 1$, die nach Induktionsvoraussetzung äquivalent zu $G_1 > G_2 > \ldots > G_r$ ist, und $t + 1 = r - 1$, analog $t + 1 = s - 1$, also $r = s$.
Wegen $G/G_1 \cong H_1/K$ und $G/H_1 \cong G_1/K$ sind die ursprünglichen Kompositionsreihen äquivalent.

4.1.7 Beispiele:

i) $\Omega = \emptyset$, Kompositionsreihen sind Subnormalketten $G = G_0 > G_1 > \ldots > G_r = (1)$ mit $G_{i+1} \trianglelefteq G_i$ und G_i/G_{i+1} einfache Gruppe.

ii) M ist R-Module, $R = K$-Algebra, $\dim_K(M) < \infty \Rightarrow M$ hat Kompositionsreihe.

iii) G ist Ω-Gruppe mit $\Omega = \mathrm{Inn}(G), G = G_0 > \ldots > G_r = (1)$ mit $G_i \trianglelefteq G$ und G_i/G_{i+1}

einfache Gruppe („Normalreihe“, Hauptreihe mit Hauptfaktoren G_i/G_{i+1})

iv) $R = \text{Ring} \ni 1, G = (R,+), \Omega = R$ operiert durch Linksmultiplikation. Kompositionsreihe: $R = R_0 > \ldots > R_r = (0)$, R_i Linksideale von R_1, R_i/R_{i+1} einfacher R-Modul.

v) $R = \text{Ring} \ni 1, M =$ abelsche Gruppe, R-Linksmodul. $M = M_0 > \ldots > M_r = (0)$ mit M_i/M_{i+1} irreduzibler R-Modul.

Beachte: Ist $G = G_0 > G_1 > \ldots > G_r$ eine Hauptreihe für G, so ist G_i/G_{i+1} minimaler Normalteiler von G/G_{i+1} (Korrespondenzsatz)

4.1.8 Satz: Ein minimaler Normalteiler einer endlichen Gruppe G ist direktes Produkt von Kopien einer einzigen einfachen Gruppe.
Beweisidee: Sei $(1) \neq N \trianglelefteq G, N \neq G$ minimaler Normalteiler von G. Ist N einfachh, so sind wir fertig.
Sei N nicht einfach und sei $(1) \neq N_1$ maximaler echter Normalteilervon N. Seien $N_1, \ldots, N_k$ die verschiedenen G-konjugierten von N_1 ($N_i = g_i N g_i^{-1}$ für ein $g_i \in G$). Nun ist $g_i N_1 g_i^{-1} \subseteq g_i N g_i^{-1} = N \Rightarrow N_1, \ldots, N_k \leq N$. Es gilt also $N_i \trianglelefteq N$
Man kann zeigen, dass alle N/N_i isomorph und einfach und $N \cong$ direktes Produkt eines Teils der N/N_i. (Details Übung)

4.1.9 Satz: Endliche Gruppen besitzen eine Hauptreihe (Kompositionsreihe mit $\Omega = \text{Inn}(G)$). Jeder Hauptfaktor ist minimale normale Untergruppe einer Faktorgruppe von G und daher direktes Produkt von Kopien einer einfachen Gruppe.
Beweis: Sei G endliche Gruppe. Induktion über $|G|$. $|G| = 1$ trivial.
Ist $(1) \neq G$ und G einfach, so ist $G > (1)$ eine Hauptreihe.
Sei also G nicht einfach und $N \neq (1)$ minimaler Normalteiler von G. Nach Induktion besitzt G/N eine Hauptreihe $G/N = G_0/N > G_1/N > \ldots > G_r/N = (1)$ mit $G_i =$ volles Urbild von $(G/N)_i$ in $G \Rightarrow G = G_0 > G_1 > \ldots > G_r = N > G_{r+1} = (1)$ ist Hauptreihe für G. □

Übung: Sei G Gruppe. Hat G eine Kompositionsreihe ($\Omega = \emptyset$), so auch eine Hauptreihe ($\Omega = \text{Inn}(G)$).

V. Lineare Darstellung

1. Grundlagen

a). Gruppenalgebren

Alle Ringe haben Einselement $1 = 1_R$, aber sind nicht notwendigerweise kommutativ.

Bekannt: Unterring, Rechts-/Linksideale (Reid, Liid), Ideale, Ringhomomorphismen, ker, im, Faktorringe, Isosätze ...

$K =$ Körper: Selbe Liste für K-Algebren.

Allgemein: $\Lambda =$ kommutativer Ring $\ni 1$, Eine Λ-Algebra is ein Ring R mit Einselement zusammen mit einem einserhaltenden Ringhomomorphsimus f von $\Lambda \to Z(R) = \{r \in R | rs = sr \forall s \in R\}$, $Z(R)$ ist immer ein Unterring von R, $1_R \in Z(R)$, so dass gilt:
(Wir schreiben Λr statt $f(\Lambda) r$ für $\lambda \in \Lambda . r \in R$)
$\lambda r = r\lambda \forall r \in R$ (f nicht notwendigerweise injektiv)
Beachte: $\overline{f} : \Lambda / \ker f \to Z(r)$ ist injektiv, d.h. R ist $\overline{\Lambda}$-Algebra mit $\overline{\Lambda} = \Lambda / \ker f$

Beachte:

i) Jeder Ring ist $\mathbb{Z}$-Algebra durch $z \mapsto z \cdot 1_R$.

ii) Unterringe einer Λ-Algebra sind nicht notwendigerweise Uneralgebren, aber Rechtsideale und Linksideale sind es. Nicht jeder Ringhomomorphsimus zwischen Λ-Algebren ist Algebra Homomorphismus (auch Λ-linear).

Beispiele:

i) $K^{n \times n}, \mathrm{End}_K(V), V = K$-Vektorraum

ii) Auf $R = \mathbb{C}^2$ definieren wir eine Multiplikation durch $(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma + \beta\delta, \alpha\delta + \beta\gamma)$
Übung: R ist 2-dimensionale kommutative $\mathbb{C}$-Algebra. $\mathbb{C}$-Basis: $\{e := (1, 0), a := (0, 1)\}$

$e \cdot e = (1,0)(1,0) = (1,0) = e, a \cdot e = e \cdot a = (0,1) = a, a \cdot a = (1,0) = e$
$(\{e,a\}, \cdot) = C_2$

5.1.1 Definition: $\Lambda =$ kommutativer Ring $\ni 1$, $A = \Lambda$-Algebra, so dass gilt:

i) Als Λ-Modul ist A frei mit einer Basis $\mathcal{B}$ so dass gilt:

ii) $(\mathcal{B}, \cdot) \cong G =$ Gruppe

iii) Dann heißt A Gruppenalgebra über Λ der Gruppe G und wird mit ΛG bezeichnet.

Fragen:

i) G Gruppe, $\Lambda =$ kommutativer Ring $\ni 1$
Gibt es eine Gruppenalgebra ΛG?

ii) Gibt es genau eine Gruppenalgebra ΛG Ja (trivial)

iii) Bestimmt die Gruppenalgebra die Gruppe G, d.h. ist $\Lambda G \cong \Lambda H \Rightarrow G \cong H$? Nein!
$|G| < \infty$. Klar $|G| = |H|$.
$\Lambda = \mathbb{C}$: Viele Gegenbeispiele: $\mathbb{C}D_8 \cong \mathbb{C}Q_8, \ldots$
$\Lambda = \mathbb{Z}$ (Highman, $\sim$ 1930) Vermutung: $\mathbb{Z}G \cong \mathbb{Z}H \Rightarrow G \cong H$? Nein, Gegenbeispiel:
$|G| = |H| = 2^21 \cdot 97^28$ (?) (Hertweck)
Es gibt kleinere! (aber nicht sehr viel kleinere)

5.1.3 Konstruktion von ΛG: Die Gruppenalgebra ΛG ist als Λ-Modul der freie Λ-Modul über der Menge G, d.h. $\Lambda G = \left\{\sum_{g \in G} \alpha_g g \mid \alpha_g \in \Lambda,\ \text{fast alle } \alpha_g = 0\right\}$
$(\sum \lambda_g g) + (\sum \mu_g g) = \sum (V + \mu_g) g$
$\beta(\sum \lambda_g g) = \sum (\beta\lambda_g) g$
$(\sum \alpha_g g)(\sum \beta_h h) = \sum_{g,h} \alpha_g \beta_h (g \cdot h) = \sum_x (\sum_{gh=x} \alpha_g \beta_h) x = \sum_x (\sum_g \alpha_g \beta_{g^{-1}x}) x$

5.1.4 Satz: Seien Λ, G, ΛG wie oben beschrieben. Dann ΛG assoziative Λ-Algebra mit Einselement $1_{\Lambda G} = \sum \alpha_g g$ mit $\alpha_g = 1$ für $g = 1$ und sonst 0. ($\alpha_g = 1_G$). Durch $g :\mapsto \sum_h a_h h$ mit $a_h = 1$ für $h = g$ und 0 sonst wird G in ΛG eingebttet und bildet eine Λ-Basis von ΛG.
Beweis: Trivial.

Andere Notation: $\sum \alpha_g g \mapsto$ Abbildung $G \to K : g \mapsto \alpha_g \in \Lambda$ mit $\alpha_g = 0$ für fast alle g.
$\Lambda G = \left\{f\ in \Lambda^G \mid f(g) = 0 \text{ für fast alle } g \in G\right\}$
$x, y \in \Lambda G \subseteq \Lambda^G$: Für $g \in G$ ist $(x+y)(g) = x(g) + y(g), (\lambda x)(g) = \lambda x(g), (xy)(g) = \sum_h x(h) y(h^{-1}g)$ „Faltung“
Erinnerung: $A = \Lambda$-Algebra, $M = A$-Linksmodul, d.h. $(M, +)$ ist abelsche Gruppe mit binärer Operation von $A \times M \to M : (a,m) \mapsto am$ mit $1_A m = m, (ab)m = a(bm), a(m+n) = am + an, (a+b)m = am + bm \forall a, b \in A, m, n \in M$

A^{mod} = Klasse der A-Linksmoduln, ${}^{mod}A$ = Klasse der Rechtsmoduln.

Definition: G = Grupoe, K = Körper. Eine (lineare)-Darstellung von G vom Grad n ist ein Homomorphismus $\rho : G \to \mathrm{GL}_n(K)$ lineare Darstellung von G über dem K-Vektorraum V ist ein Homomorphismus $\varphi : G \to \mathrm{Aut}_k(V)$.

Klar:

$$\begin{array}{ccccc} G & \xrightarrow{\varphi} & \mathrm{Aut}_K(V) & \xrightarrow[\text{Wahl der Basis}]{\sim} & \mathrm{GL}_n(K) \quad n = \dim_V(K) \\ \downarrow & & \downarrow & & \downarrow \\ KG & \longrightarrow & \mathrm{End}_K(V) & \xrightarrow[\text{Wahl der Basis}]{\sim} & M_{n\times n}(K) \end{array}$$

Für eine K-Algebra A ist eine Darstellung von A über dem K-Vektorraum V ein K-Algebra-Homomorphismus $A \to \mathrm{End}_K(V) \cong M_{n\times n}(K)(\dim_K V = n)$
Sei $\rho : KG \to \mathrm{End}_K(V)$ Darstellung. Dann wird V zum KG-Modul durch $x \cdot m = (\rho(x))(m)$ für $y \in KG$ und $m \in V$.
Umgekehrt: Ist V ein A-Modul, so wird durch $\rho : A \to \mathrm{End}_K(V) : a \mapsto \lambda_a, \lambda_a(v) = av$ für $a \in A, v \in V$ eine Darstellung von A über V definiert.
So: Konzept der Darestellungen von A ist äquivalent zum Konzept der A-Moduln. (Vgl. Permutationsdarstellungen).
Homomorphismen von A-Moduln: Klar.
Homomorphismen von Darstellungen: Seien $\rho : A \to \mathrm{End}_K(V), \psi : A \to \mathrm{End}_K(W)$ Darstellungen von A. Ein Homomorphismus von ρ nach ψ ist ein K-lineare Abbildung $f : V \to W$, so dass $\forall a \in A : f \circ \rho(a) = \psi(a) \circ f$

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \rho(a)}\downarrow & & \downarrow{\scriptstyle \psi(a)} \\ V & \xrightarrow{f} & W \end{array}$$

Beachte: $W = V$ mit $f \in \mathrm{Aut}_K(V)$ Homomorphismus von ρ nach $\psi \Leftrightarrow \psi(a) = f \circ \rho(a) \circ f^{-1} \forall a \in A$
$\dim_K(V) = n, \tilde{\rho} : A \to M_{n\times n}(K), \tilde{\psi} : A \to M_{n\times n}(K)$ zugehörige Matrixdarstellungen nach Wahl einer Basis $\mathcal{B}$, so kann man f als Basiswechsel interpretieren: $m_{\mathrm{id}}(\mathcal{C}, \mathcal{B}) = m_f(\mathcal{B}, \mathcal{B})$ für Basis $\mathcal{C}$ von V.
$m_{\tilde{\psi}}(\mathcal{C}, \mathcal{C}) = m_{\mathrm{id}}(\mathcal{C}, \mathcal{B}) m_{\tilde{\rho}}(\mathcal{B}, \mathcal{B}) m_{\mathrm{id}}(\mathcal{B}, \mathcal{C})$ (Details: Übung)

Definition: Seien A, B Λ-Algebren mit 1 und sei M ein A-Linksmodul und ein B-Rechtsmodul. M heißt A-B-Bimodul falls gilt:
$\forall \alpha \in A, \beta \in B, m \in M : (\alpha m)\beta = \alpha(m\beta)$
(M A-Linksmodul und B-Linksmodul: $\alpha(\beta m) = \beta(\alpha m)$)

Beachte: Für die zugehörigen Darstellungen bedeutet das: $\lambda_\alpha : M \to M : m \mapsto \alpha m, \rho_\beta : M \to M : m \mapsto m\beta$
(Abbildung $\rho : B \to \mathrm{End}_\Lambda(M)$ ist Antihomomorphismus, d.h. $\rho_\beta\rho_\gamma = \rho_{\gamma\beta}$ für $\gamma, \beta \in B$)
Bedingung $\Leftrightarrow \lambda_\alpha\rho_\beta = \rho_\beta\lambda_\alpha \forall \alpha \in A, \beta \in B$
d.h. λ_α und ρ_β zentralisieren einander in $\mathrm{End}_\Lambda(M)$ ($\forall \lambda \in \Lambda, m \in m : \lambda m = m\lambda$)

5.1.3 Beispiel: $M \in A^{mod} = \{$Links-A-Moduln$\}$. Sei $E = \mathrm{End}_A(M)$. E operiert auf M von rechts.
$E = \{b \in \mathrm{End}_\Lambda(M) \mid (am)b = a(mb) \forall a \in A, m \in M\}$
Dann ist E Λ-Algebra und M ein A-E-Bimodul.
Beweis: $A = \Lambda$-Algebra $\Rightarrow$ M ist Λ-Modul durch Einschränken, $\lambda m = (\lambda 1_A)m$. Durch $\lambda m = m\lambda$ wird M ein Λ-Rechtsmodul, da Λ kommutativ ist.
Ein A-Endomorphismus ist dann auch ein Λ-Endomorphismus, d.h. $E = \mathrm{End}_A(M) \subseteq \mathrm{End}_\Lambda(M)$.

(Beachte: $\{\mathbb{Z}$-Moduln$\} = \{\mathbb{Z}$-Bimoduln$\} = \{$abelsche Gruppen$\}$)

Für $b \in E$, $m \in M$ und $\lambda \in \Lambda$ sei $\lambda b \in \mathrm{End}_A(M)$ definiert durch $m(\lambda b) = \lambda(mb) = (mb)\lambda = m(b\lambda)$. So ist E eine Λ-Algebra. Rest klar.

Bemerkung: A und B seien Λ-Algebren, M ein A-Links- und B-Rechtsmodul. $\lambda : A \to \mathrm{End}_\Lambda(M) : a \mapsto \lambda_a, \rho : B \to \mathrm{End}_\Lambda(M) : b \mapsto \rho_b, \rho_b(m) = mb$
ρ Antihomomorphismus, λ Homomorphismus von Λ-Algebra
$\tilde{B} = \mathrm{im}\,\rho \subseteq \mathrm{End}_\Lambda(M) \supseteq \tilde{A} = \mathrm{im}\,\lambda$

(R Ring, R^{opp} = Ring auf Menge R mit Multiplikation $*$ gegeben durch $r * s = sr \forall r, s \in R$)

Dann ist M ein A-B-Bimodul $\Leftrightarrow \tilde{B} \subseteq \mathrm{End}_A(M) \subseteq \mathrm{End}_\Lambda(M) \Leftrightarrow \tilde{A} \subseteq \mathrm{End}_B(M) \subseteq \mathrm{End}_\Lambda(M)$

Man sagt: M erfüllt Schur-Wyl-Dualität oder ist balanced oder erfüllt Bizentralisatoren Eigenschaft, falls gilt: $\tilde{B} = \mathrm{End}_A(M), \tilde{A} = \mathrm{End}_B(M)$.

$\rightsquigarrow$ Ausrechnen von $\mathrm{End}_A(M) : \Lambda = K$ Körper, $M \in \Lambda^{mod}, \dim_K M = n < \infty, \rho : A \to M_{n\times n}(K)$ zugehörige Matrixdarstellung.
$G_a : \rho(a)X = X\rho(a), X \in M_{n\times n}K$. Um E auszurechnen genügt es die Gleichunssysteme G_a für $a \in A$ simultan zu lösen.
Angenommen, $a_1, \ldots, a_k \in A$ so, dass A die kleinste Unteralgebra von A ist, die $a_1, \ldots, a_k$ enthält, d.h. $\{a_1, \ldots, a_k\}$ erzeugt die K-Algebra A, dann genügt es $\rho(a_i)X = X\rho(a_i)$ simultan zu lösen $\rightsquigarrow$ mühsamer Weg um E auszurechnen.

b). Tensorprodukte

A, B, C seien Λ-Algebren, Λ kommutativer Ring $\ni 1$. ${}_A\mathrm{mod}_B := \{A\text{-}B\text{-Bimoduln}\}$

Definition: Sei $M \in {}_A\mathrm{mod}_B, N \in {}_B\mathrm{mod}_C$. Eine Abbildung $f : M \times N \to U \in {}_A\mathrm{mod}_C$ heißt A-C-bilinear und B-balanced, falls gilt $\forall a \in A, b \in B, c \in C, m, m_1, m_2 \in M, n, n_1, n_2 \in N$:

i) f ist bilinear, d.h. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n), f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$

ii) $f(am, n) = af(m, n)$

iii) $f(m, nc) = f(m, n)c$

iv) $f(mb, n) = f(m, bn)$

Ein Tensorprodukt $M \otimes_B N \in {}_A\mathrm{mod}_C$ über B ist ein A-C-Bimodul zusammen mit einer A-C-bilinearen, B-balanced Abbildung $\eta : M \times N \to M \otimes_B N$ so, dass folgende universelle Eigenschaft gilt:

$$\begin{tikzcd} M \times N \arrow[r, "\eta"] \arrow[dr, "f"'] & M \otimes_B N \arrow[d, "\exists ! \hat{f}"] \\ & U \in {}_A\mathrm{mod}_C \end{tikzcd}$$

mit $\hat{f} \circ \eta = f$

$\mathcal{A}$ = freie abelsche Gruppe über
$M \times N = \{z_1(m_1, n_2) + z_2(m_2, n_2) + \ldots + z_k(m_k, n_k) \mid m_i \in M, n_i \in N, k \in N, z_i \in \mathbb{Z}\}$
$I = \{(m_1 + m_2, n) - (m_1, n) - (m_2, n), (m, n_1 + n_2) - (m, n_1) - (m, n_2), (mb, n) - (m, bn)\}$
$(b \in B, m, m_1, m_2 \in M, n, n_1, n_2 \in N)$

$\mathcal{A}$ ist A-Linksmodul durch $a(\sum z_i(m_i, n_i)) = (\sum z_i(am_i, n_i))$, C-Rechtsmodul analog.
$cA \in {}_A\mathrm{mod}_C$, I ist A-C-invariant $\Rightarrow < I >$ ist A-C-Unterbimodul.
$M \otimes_B N = A/ < I > \in {}_A\mathrm{mod}_C$
$\eta : M \times N \to M \otimes_B N : (m, n) \mapsto (m, n)+ < I >= m \otimes n$ (einfacher Tensor)
Klar: $\{m \otimes n \mid m \in M, n \in N\}$ erzeugt $M \otimes_B N$, d.h.
$M \otimes_B N = \left\{\sum_{i=1}^k m_i \otimes n_i \mid m_i \in M, n_i \in N, k \in \mathbb{N}\right\}$

Bemerkung: $M \in {}_A\mathrm{mod}_B \subseteq \mathrm{mod}_B, N \in {}_B\mathrm{mod}$.
Bilde $M \otimes_B N$ mit M nur als B-Rechtsmodul. $\tilde{X} = M \otimes_B N$ mit M als A-B-Bimodul.

Dann ist $X \in {}_A\text{mod}$ und $X \cong \tilde{X}$ als A-Linksmodul.

Für $a \in A$ definiere eine Abbildung $f_a : M \times N \to M \times N : (m,n) \mapsto (am, n)$
A-$\mathbb{Z}$-bilinear, B-balanced (wegen $(am)b = a(mb)$, da M A-B-Bimodul).

$$\begin{tikzcd} M \times N \arrow[r, "\eta"] \arrow[dr, "f_a"'] & M \otimes_B N \arrow[d, "\exists! \hat{f}_a"] \\ & M \otimes_B N \end{tikzcd}$$

mit $\hat{f}_a(\sum m_i \otimes n_i) = \sum am_i \otimes n_i$

5.2.1 Fakten:

i) $M \in {}_A\text{mod}, A \in {}_A\text{mod}_A \Rightarrow A \otimes_A M \cong M$
Beweis: $f(a,m) = am$

$$\begin{tikzcd} A \times M \arrow[r, "\eta"] \arrow[dr, "f"'] & A \otimes_A M \arrow[d, "\hat{f}"] \\ & M \end{tikzcd}$$

$\hat{f}(\sum a_i \otimes m_i) = \sum a_i m_i \in M, \hat{f}^{-1} : M \to A \otimes_A M : m \mapsto 1_A \otimes m \in A \otimes M$

ii) Tensorprodukte vertauschen mit direkten Summen: $(\oplus_{i\in I}) \otimes_A N \cong \oplus_{i \in I}(M_i \otimes N)$
$M \cong \oplus_{i\in I} A_i, A_i \cong_A A, N \in {}_A\text{mod}$
$M \otimes_I N = (\oplus_{i \in I} A_i) \otimes N \cong \oplus_{i\in I}(A_i \otimes N) \cong N = \oplus_{i \in I} N_i$ mit $N_i \cong N$ als A-Modul.

iii) $({}_A M \otimes_B N) \otimes_C L_D \cong {}_A M \otimes_B (N \otimes_C L)_D$ Assoziativität, $N \in {}_B\text{mod}_C$

Beispiel: $X := \mathbb{Z}/z\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = (0)$
$1 = 2 \cdot 2 - 3$
$a \otimes b \in X : a \otimes b = 1a \otimes b = (4-3)(a \otimes b) = 4(a \otimes b) - 3(a \otimes b) = (4a) \otimes b - a \otimes (3b) = 0 \otimes b - a \otimes 0 = 0$

5.2.2 Wichtiges Beispiel: K Körper, G Gruppe, $H \leq G$. $M \in {}_{KH}\text{mod}$
Beachte: $KG \in {}_{KG}\text{mod}_{KH}$
So: $KG \otimes_{KH} M \in {}_{KG}\text{mod}$
Wir schreiben: $\text{Ind}_H^G M =$ der von H nach G induzierte Modul.

Seien $M, N \in {}_{KH}\text{mod}, f : M \to N$ KH-linear. Dann ist $\text{id}_{KG} \otimes f : KG \otimes_{KH} M \to KG \otimes_{KH} N$ KG-linear.

5.2.3 Lemma: Seien $M_1, M-2 \in {}_R\text{mod}_S$, R, S, T Λ-Algebren, $N_1, N_2 \in {}_S\text{mod}_T$, $f : M_1 \to M_2$ R-S-linear, $g : N_1 \to N_2$ S-T-linear.
Dann wird durch $f \otimes g : M_1 \otimes_S N_1 \to M_2 \otimes_S N_2 : m \otimes n \mapsto f(m) \otimes g(n)$ eine R-T-lineare Abbildung definiert.
Beweis: Wir definieren Abbildung $f \times g : M_1 \times N_1 \to M_2 \otimes_S N_2 : (m, n) \mapsto f(m) \otimes g(n)$.
Leicht: $f \times g$ ist R-T-linear und S-balanced. $((f \times g)(rm, n) = f(rm) \otimes (g(n) = r(f(m) \otimes g(n)), (f \times g)(ms, n) = f(ms) \otimes g(n) = f(m)s \otimes g(n) = f(m) \otimes sg(n) = f(m) \otimes g(sn) = (f \times g)(m, sn))$

$$\begin{tikzcd} M_1 \times N_1 \arrow[r, "\eta"] \arrow[dr, "f \times g"'] & M_1 \otimes N_1 \arrow[d, "\exists!\,\widehat{f \times g} = f \otimes g"] \\ & M_2 \otimes N_2 \end{tikzcd}$$

$\square$

Sei $\{g_i \mid i \in I\}$ Vertretersystem der Linksnebenklassen von H in G, d.h. $G = \dot{\bigcup\limits_{i \in I}} g_i H$. Sei $g \in G$, dann $\exists! i \in I, h \in H : g = g_i \cdot h$.
Also lässt sich jedes $x \in KG$ eindeutig als Linearkombination $x = \sum_{i \in I} g_i y_i$ mit $y_i \in KH$ (fast alle 0) schreiben. $(x = \sum_{g \in G} \lambda_g \cdot g = \sum_{i \in I} g_i (\sum_{h \in H} \lambda_{g_i h} h), \lambda_g \in K$ fast alle 0)

Also: $KG_{KH} = \oplus_{i \in I} g_i KH$, ($KH$-Rechtsuntermoul von $KG_{KH}, g_i KH \cong KH$ als KH-Rechtsmodul)
KG_{KH} ist frei als KH-Modul, mit KH-Basis g_i.
Nun ist $g_i H \otimes_{KH} M = g_i \otimes_{KH} M$
Wir haben gezeigt: $\text{Ind}_{KH}^{KG} M = KG \otimes_{KH} M \cong \oplus_{i \in I} g_i \otimes M$ (mit $g_i \otimes M \cong M$ als K-Vektorraum) $\cong \oplus |I|$ vielen Kopien vn KH als Vektorraum.
($g_i \otimes M$ ist ein $g_i KH g_i^{-1}$-Modul)

Allgemein: $S \subseteq R$ Ringe, $M \in {}_S\text{mod}$, ${}_R R_S \in {}_R\text{mod}_S, \text{Ind}_S^R = R \otimes_S M \in {}_R\text{mod}$
Im allgemeinen ist aber R_S nicht frei. Es kann durchaus passieren, dass $R \otimes_S M = (0)$.

5.2.4 Lemma: Sei A, B K-Algebren, K Körper. Dann wird $A \otimes_K B$ zur K-Algebra vermöge der folgenden Multiplikation:
$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$
Problem: Ist diese Multiplikation wohldefiniert?
Beweis: Übung

5.2.5 Korrolar: Seien $M \in {}_A\text{mod}, N \in {}_B\text{mod}$. Dann wird $M \otimes_K N$ ein $A \otimes_K B$-Modul durch:
$(a \otimes b)(m \otimes n) = am \otimes bn$

5.2.6 Beobachtung: Sind G, H Gruppen, so ist $K(G \times H) \cong KG \otimes_K KH$

Beweis: $LAAG \Rightarrow KG \otimes_K KHG$ hat Basis $\mathcal{B} = \{g \otimes h \mid g \in G, h \in H\}$
$(g_1 \otimes h_1)(g_2 \otimes h_2) = (g_1 g_2) \otimes (h1 h_1)$
$\Rightarrow \mathcal{B}$ ist Gruppenbasis von $KG \otimes_K KH, \mathcal{B} \cong G \times H$ als Gruppe $\square$

Ist X Grupe, $f : X \to G \times H$ Gruppenhomomorphismus. So kann dieser zu einem K-Algebrahomomorphismus $f : KX \to KG \otimes_K KH$ fortgesetzt werden.

5.2.7 Definition: Sei G Gruppe, dann wird durch $\Delta g = (g, g) \in G \times G$ ein injektiver Gruppenhomomorphismus $\Delta : G \to G \times G$ definiert. Es ist $\Lambda(\sum \lambda_g g) = \sum \lambda_g (g \otimes g)$. Sind $M, N \in {}_{KG}\text{mod}$, so wird $M \otimes_K N$ ein KG-Modul durch Einschränken auf der $KG \otimes_K KG$-Operation aus 5.2.5 auf $M \otimes_K M$ auf $\operatorname{im} \Delta \cong G$. So gilt: $g \in G, m \in M, n \in N$ ist $g(m \otimes n) = gm \otimes gn$.
Vorsicht: Sei $x = \sum \lambda_g g \in KG, m \in M, n \in N$:
$x(m \otimes n) = (\sum \lambda_g g)(m \otimes n) = \sum \lambda_g (gm \otimes gn)$
$xm \otimes xn = (\sum \lambda_g gm) \otimes (\sum \lambda_h hn) = \sum\limits_{g \in G, h \in H} \lambda_g \lambda_h (gm \otimes hn)$
Also ist i.A. $x(m \otimes n) \neq xm \otimes xn$

c). KG-Moduln Grundlagen

$A = K$-Algebra, K Körper, $M \in {}_A\text{mod}$. Ist $m \in M$, so ist $A \cdot m = \{a \cdot m \mid a \in A\}$ ein A-Untermodul.
Ist $S \subseteq M$, so ist $< S >=< S >_{A\text{-Modul}} = \sum_{s \in S} As \leq M$ der von S erzeugte Untermodul von M.
$< S >= \bigcap_{U \leq M, s \leq U} U =$ kleinste Untermodul von M, der S enthält. $S \subseteq M$ heiß Erzeugendensystem von M falls $< S >= M$.
M heißt endlich erzeugt, falls M ein endliches Erzeugendensystem hat.
M heißt zyklischer A-Modul, falls $M = A \cdot m$ für ein $m \in M$.

5.3.1 Satz: Sei $M \in {}_A\text{mod}$. Dann ist M zyklisch $\Leftrightarrow$ M ist epimorphes Bild von ${}_AA \in {}_A\text{mod}$.
Beweis: „$\Rightarrow$“: Sei $M = Am$ zyklischer Modul. Definiere $f : {}_AA \to m : a \mapsto a \cdot m$. f ist A-linear: $f(ba) = (ba)m = b(am) = bf(a), f(a + b) = (a + b)m = am + bm = f(a) + f(b)$.
Klar: Wegen $M = Am$ ist f Epimorphismus von ${}_AA$ auf M. $M \cong {}_AA / \ker f, \ker f = \{a \in A \mid am = 0\} = ann_A(m)$.
„$\Leftarrow$“: Sei $f : {}_AA \to M$ Epimorphismus, $m = f(1)$. Sei $x \in M, a \in A : f(a) = x$
Dann ist $x = f(a) = f(a \cdot 1) = af(1) = am$. Also ist $M = Am$ zyklischer Modul.

Beispiel: $M \in {}_A\text{mod}$ irreduzibel, $0 \neq m \in M$. $(0) \neq Am \leq M \Rightarrow Am = M \Rightarrow M$ zyklisch.

5.3.2 Satz: Sei A endlich dimensionale K-Algebra und sei $M \in {}_A\text{mod}$ endlich erzeugt. Dann ist $\dim_K M < \infty$ und M besitzt eine Kompositionsreihe.
Beweis: $M = \sum_{i=1}^{k} Am_i, \exists m_i \in M, k \in \mathbb{N}$

Am_i ist zyklischer Modul und daher epimorphes Bild von ${}_AA$. Wegen $\dim_K({}_AA) < \infty$ ist $\dim_K(Am_i) < \infty$, und daher $\dim_K M \leq \sum_{i=1}^k \dim_K(Am_i) < \infty$.
Da jeder A-Untermodul von M insbesondere ein K-Untervektorraum von M ist, muss jede echt absteigende Kette von A-Untermoduln von M terminieren. Also hat M eine Kompositionsreihe und Jordan-Hölder gilt. □

5.2.3 Korrolar: Sei A K-Algebra. Dann ist jeder einfache A-Modul zyklisch und daher epimorphes Bild vom regulären A-Modul ${}_AA$. Ist insbesondere $\dim_K A < \infty$, so sind alle irreduziblen A-Moduln endlich dimensional. Wegen $\dim_K A < \infty$ hat ${}_AA$ eine Kompositionsreihe und daher kommen nur endlich viele Kompositionsfaktoren vor. Also gibt es nur endliche viele nicht isomorphe irreduziblen A-Moduln.
Beweis: Sei $M \in {}_A\mathrm{mod}$ irreduzibel, und sei $M \neq (0)$. Sei $0 \neq m \in M \Rightarrow M = A \cdot m$, da $0 \neq Am \leq M$ und M irreduzibel. Also ist $Am = M$, d.h. M ist zyklisch. Rest folgt. □

Bemerkung: Es ist im Allgemeinen falsch, dass jeder irreduzible A-Modul als Untermodul von ${}_AA$ vorkommt! Für Gruppenalgebren KG, $|G| < \infty$, stimmt dies aber!

Beispiele von KG-Moduln:

i) ${}_{KG}KG$ ist der reguläre KG-Modul. Die zugehörige (Matrix-)Darstellung $\rho : G \to M_{|G|\times|G|}(K)$:
$\mathcal{B} = G =$ Basis von ${}_{KG}KG$ geordnet
Sei $g \in G$. Dann ist $g \cdot h \in G$ für ein $h \in G$. Man erhält die Permutationsmatrix, die die Linksmultiplikation von g auf G darstellt.

ii) Allgemeiner: Sei Ω endliche G-Menge, und sei $\rho : G \to \sigma_\Omega$ die zugehörige Permutationsdarstellung. Ordne $\Omega = \{\omega_1, \ldots, \omega_k\}$.

$$\begin{array}{lll} \rho : G & \longrightarrow \sigma_k & \cong W \leq \mathrm{GL}_n(K) \\ \quad \downarrow & & \\ KG & \longrightarrow M_{k\times k}(K) & \end{array}$$

Modul: $V =$ (freie) K-Vektorraum mit Basis $\Omega, \sigma_\Omega \subseteq \mathrm{End}_K(V)$
$\rho : KG \to \mathrm{End}_K(V) : g \mapsto$ Permutationsmatrix. $V \in {}_{KG}\mathrm{mod}$ „Permutationsmodul“

iii) Der triviale KG-Modul ist K mit G-Operation $g \cdot \lambda = \lambda \forall g \in G, \lambda \in K$.
Das heißt G operiert „trivial“ auf K. Die zugehörige Darstellung ist gegeben als Gruppenhomomorphismus $G \to K^* : g \mapsto 1_K$ bzw. $\rho : KG \to K : \sum \lambda_g g \mapsto \sum \lambda_g$, fast alle $\lambda_g = 0$ (Epimorphismus).
Es ist der $\ker \rho =< g - 1 \mid g \in G >_{\text{Ideal}} \trianglelefteq KG$.
(Für $S \subseteq A = K$-Algebra: $< S >_A = \bigcap_{I \trianglelefteq A, S \subseteq I} I =$ kleinstes Ideal von A, das S als Teilmenge enthält $= \sum_{s\in S} AsA$)
$\dim_K(\ker \rho) = |G| - 1$

Das Ideal $< g-1 \mid g \in G >_{\text{Ideal}}$ heißt Augmentationsideal von G und wird mit ΩKG bezeichnet.

iv) Sei $H \leq G$, ${}_HK$ triviale KH-Modul, $G = \dot{\bigcup\limits_{i\in I}} g_iH, \{g_i \mid i \in I\}$ Vertretersystem von H-Linksnebenklassen in G.
G operiert auf $G\backslash H = \{g_i \mid i \in I\}$ durch Linkstranslation: Für $g \in G, i \in I$ gibt es genau ein $j \in I$ und $h \in H : gg_i = g_jh$
$g \cdot g_i \Rightarrow g_j$ ist Permutationsdarstellung.
Sei V der K-Vektorraum mit Basis $g_i, i \in I$. Dann wird V zum KG-Modul nach ii).
$\varphi : KG \otimes_{KH} K \Rightarrow V : \sum_{i\in I} \alpha_i g_i \otimes 1_k \mapsto \sum_{i\in I} \alpha_i g_i$, d.h. Permutationsmodul von der G-Menge $G\backslash H$ ist $KG \otimes_{KH} K = \text{Ind}_{KH}^{KG}({}_HK)$

Umgekehrt: Ist Ω eine G-Menge und ohne Einschränkung transitiv (disjunkte Vereinigung von Orbits $\leftrightarrow$ direkte Summe der zugehörigen Permutationsmodule).
Sei $\Omega = (\omega_1, \ldots, \omega_k), H = \text{Stab}_G(\omega_1)$. Dan ist der Permutationsmodul nach ii) isomorph zu $KG \otimes_{KH} K = \text{Ind}_H^G({}_HK)$.

v) Sei $V \in {}_{KG}\text{mod}, V^* = \text{Hom}_K(V, K)$. Dann wird V^* zum KG-Modul durch $f \in V^*, g \in G, v \in V : (gf)(v) := f(g^{-1}v)$.
D.h. für fast alle $\lambda_g = 0$: $((\sum \lambda_g g)f)(v) = \sum \lambda_g f(g^{-1}v) \in K$

5.2.4 Lemma: Sei $A, B, C, D, \ldots$ K-Algebren, ${}_AM_B \in {}_A\text{mod}_B$, ${}_AN_C \in {}_A\text{mod}_C$. Dann wird $F := \text{Hom}_A({}_AM_B, {}_AN_C) \in {}_B\text{mod}_C$ durch:
$(bf)(m) := f(mb), (fc)(m) := f(m)c$
Analog: Ist $M \in {}_A\text{mod}_B, N \in {}_C\text{mod}_B \Rightarrow F := \text{Hom}_B({}_AM_B, {}_CN_B) \in {}_C\text{mod}_A$ durch:
$(cfa)(m) := c \cdot f(am)$
Beweis: bf ist wohldefinierte Abbildung von $M \to N$. Zu zeigen: bf ist A-linear:
$(bf)(m_1+m_2) = f((m_1+m_2)b) = f(m_1b+m_2b) = f(m_1b)+f(m_2b) = (bf)(m_1)+(bf)(m_2)$
$(bf)(am) = f((am)b) = f(a(mb)) = a \cdot f(mb) = a \cdot (bf)(m)$
Weiter ist z.Bsp:
$((b_1b_2)f)(m) = f(m(b_1b_2)) = f((mb_1)b_2) = (b_2f)(mb_1) = (b_1(b_2f))(m)$ usw. (Übung)
Also ist $\text{Hom}_A(M, N)$ ein Links-B-Modul, jetzt Rechts-C-Modul: $(fc)(m_1+m_2) = f(m_1+m_2)c = (f(m_1)+f(m_2))c = f(m_1)c + f(m_2)c = (fc)(m_1) + (fc)(m_2)$
$(fc)(am) = f(am)c = (a \cdot f(m))c = a(f(m)c) = a(fc)(m)$
$(f(c_1c_2))(m) = f(m)(c_1c_2) = (f(m)c_1)c_2 = (fc_1)(m)c_2 = ((fc_1)c_2)(m)$ usw.
und: $((bf)c)(m) = ((bf)(m))c = (f(mb))c = (fc)(mb) = (b(fc))(m)$, damit ist $\text{Hom}_A(M, N)$ ein B-C-Bimodul. □

Beispiel: $V \in {}_A\text{mod} \Rightarrow V^* \in \text{mod}_A, V^* = \text{Hom}_K({}_AV_K, K_K) \in \text{mod}_A$
$f \in V^*, a \in A : (fa)(v) = f(av)$

5.2.5 Lemma: Sei A K-Algebra, $\iota : A \to$ Antihomomorphismus von K-Algebren, d.h. ι ist K-linear, $\iota(a_1a_2) = \iota(a_2)\iota(a_1)$.

Sei $V \in {}_A\mathrm{mod}$. Dann wird $V \in \mathrm{mod}_A$ durch $v.a = \iota(a)v$
Beweis: $v.(a_1 + a_2) = \iota(a_1 + a_2)v = \iota(a_1)v + \iota(a_2)v = v.a_1 + v.a_2$ und
$v.(a_1a_2) = \iota(a_1a_2)v = \iota(a_2)\iota(a_1)v = \iota(a_2)(va_1) = (va_1).a_2$ usw. $\square$

5.2.6 Lemma: Sei G Gruppe. Dan induziert $g \mapsto g^{-1}$ einen Antihomomorphismus von KG in KG ($\sum \lambda_g g \mapsto \sum \lambda_g g^{-1}$).

5.2.7 Korrolar: $V \in {}_{KG}\mathrm{mod}$. Dann wird $V^* = \mathrm{Hom}_K(V, K)$ zum KG-Modul durch $(gf)(v) := f(g^{-1}v)$.

5.2.8 Korrolar: Seien $V, W \in {}_{KG}\mathrm{mod}$. Dann wird $\mathrm{Hom}_K(V, W)$ zum KG-Modul durch $(g.f)(v) := gf(g^{-1}v)$
(Da $\mathrm{Hom}_K({}_{KV}V_K, {}_{KG}W_K) \in {}_{KG}\mathrm{mod}_{KG}$)
Beweis: $\mathrm{Hom}_K({}_{KG}V, {}_{KG}W) \in {}_{KG}\mathrm{mod}_{KG}$ durch $(gfh)(v) = gf(hv)$ für $f \in \mathrm{Hom}_K(V, W), g, h \in G, v \in V$. Also ein $KG \otimes_K KG^{op}$-Modul.
Mit $\Delta : G \Rightarrow G \times G^{op} : g \mapsto (g, g^{-1})$ wird daher $\mathrm{Hom}_K(V, W)$ zum Links-KG-Modul durch Einschränken.
$(g \otimes g^{-1})f = gfg^{-1}$
Beachte: $(g.f)(v) = g(f(g^{-1}v)) \Rightarrow ((g_1, g_2).f)(v) = (g_1g_2)(f(g_2^{-1}g_1^{-1}v)) = g_1(g_2f(g_2^{-1}(g_1^{-1}v))) = g_1((g_2f)(g_1^{-1}v)) = (g_1.g_2.f)(v)$

5.2.9 Definition und Lemma: Sei $M \in {}_{KG}\mathrm{mod}$. Dann ist $M^G = \{m \in M \mid gm = m \forall g \in G\}$ der größte Untermodul von M, auf dem G trivial operiert. M^G ist direkte Summe von $\dim_K(M^G)$ vielen Kopien des trivialen G-Moduls K. Die ELemente von M^G werden G-Invarianten genannt.
Beweis: leicht.
$(i \mid i \in I)$ K-Basis von $M^G \Rightarrow M^G = \bigoplus_{i \in I} Kv_i, Kv_i \cong K =$ trivialer KG-Modul $\square$

5.2.10 Satz: Sei $M, N \in {}_{KG}\mathrm{mod}$ und sei $\mathrm{Hom}_K(M, N) \in {}_{KG}\mathrm{mod}$ wie in 5.2.8. Dann ist $\mathrm{Hom}_K(M, N)^G \cong \mathrm{Hom}_{KG}(M, N)$ (als K-Vektorraum).
Beweis: Sei $f \in \mathrm{Hom}_K(M, N)$. Dann ist $f \in \mathrm{Hom}_K(M, N)^G \Leftrightarrow g.f = f \forall g \in G \Leftrightarrow (g.f)(v) = f(v) = gf(g^{-1}v) \forall g \in G, v \in M \Leftrightarrow f(gv) = gf(v) \Leftrightarrow f \in \mathrm{Hom}_{KG}(M, N)$

5.2.11 Satz: Sei $U, V \in {}_{KG}\mathrm{mod}$ endlicher Dimension. Dann ist $\mathrm{Hom}_K(U, V) \cong U^* \otimes V$ als KG-Moduln.

Spezialfall: $U = V, \dim_K(V) < \infty$. Dann ist $\mathrm{End}_{KG}(V) \cong (V^* \otimes V)^G$ als K-Vektorraum.

Beweis 5.2.11: U^* ist G-Modul durch: $\alpha \in U^* : (g\alpha)(u) = \alpha(g^{-1}u)$ (siehe weit oben), und daher wird $U^* \otimes V$ zum G-Modul durch $g(\alpha \otimes v) = (g\alpha) \otimes (gv)$.
Definiere $\Gamma : U^* \otimes_K V \to \mathrm{Hom}_K(U, V)$ durch $\alpha \otimes v \mapsto A_{\alpha,v}$ mit $A_{\alpha,v}(u) := \alpha(u) \cdot v \in V$.
Klar ist: $A_{\alpha,v}$ ist Abbildung $U \to V$. Zu zeigen: $A_{\alpha,v}$ ist K-linear:
$A_{\alpha,v}(u_1 + u_2) = (\alpha(u_1 + u_2))v = (\alpha(u_1) + \alpha(u_2))v = \alpha(u_1)v + \alpha(u_2)v = A_{\alpha,v}(u_1) + A_{\alpha,v}(u_2)$
$A_{\alpha,v}(\lambda u) = \lambda A_{\alpha,v}(u)$ ebenso. So ist $A_{\alpha,v} \in \mathrm{Hom}_K(U, V)$.

Definiere $\hat{\Gamma} : U^* \times V \to \mathrm{Hom}_K(U,V) : (\alpha, v) \mapsto A_{\alpha,v}$
$\hat{\Gamma}(\alpha_1+\alpha_2, v)(u) = A_{\alpha_1+\alpha_2,v}(u) = ((\alpha_1+\alpha_2)(u))v = (\alpha_1(u)+\alpha_2(u))v = \alpha_1(u)v + \alpha_2(u)v = A_{\alpha_1,v}(u) + A_{\alpha_2,v}(u) = (A_{\alpha_1,v} + A_{\alpha_2,v})(u)$
$\Rightarrow \hat{\Gamma}(\alpha_1+\alpha_2, v) = \hat{\Gamma}(\alpha_1, v) + \hat{\Gamma}(\alpha_2, v)$
Ähnlich $\hat{\Gamma}(\alpha, v_1+v_2) = \hat{\Gamma}(\alpha, v_1) + \hat{\Gamma}(\alpha, v_2)$, also $\hat{\Gamma}$ bilinear.
$\lambda \in K : \hat{\Gamma}(\alpha\lambda, v)(u) = A_{\alpha\lambda,v}(u) = (\alpha\lambda)(u)(v) = \alpha(u)\lambda v = A_{\alpha,\lambda v}(u) = \hat{\Gamma}(\alpha, \lambda v)$, also ist $\hat{\Gamma}$ auch K-balanced. Daher ist (universelle Eigenschaft) Γ wohldefinierte K-lineare Abbildung.

Ist $(u_1, \dots, u_n)$ K-Basis von U und $(u_1^*, \dots, u_n^*)$ duale Basis $(u_i^*(u_j) = \delta_{ij})$, so kann jedes Element von $U^* \otimes_K V$ eindeutig als Summe $\sum_{i=1}^n u_i^* \otimes x_i$ mit $x_i \in V$ geschrieben werden.
$(U^* = \bigoplus_{i=1}^n Ku_i^* \Rightarrow U^* \otimes_K V \cong \bigoplus_{i=1}^n (u_i^* \otimes V))$
Sei $1 \leq j \leq n : \Gamma(\sum_{i=1}^n u_i^a st \otimes x_i)(u_j) = \sum_{i=1}^n \Gamma(u_i^* \otimes x_i)(u_j) = \sum u_i^*(u_j)x_i = x_j$
So $\Gamma(\sum_{i=1}^n u_i^* \otimes x_i) = 0 \Leftrightarrow x_j = 0 \forall j \Leftrightarrow \sum_{i=1}^n u_i^* \otimes x_i = 0 \Rightarrow \Gamma$ injektiv.
Wegen $\dim_K(U^* \otimes V) = \dim_K(U^*) \cdot \dim_K(V) = \dim_K(U) \cdot \dim_K(V) = \dim_K(\mathrm{Hom}_K(U,v))$ ist Γ ein K-Isomorphismus.

Bleibt zu zeigen: Γ ist G-linear. $g \in G, \alpha \in U^*, v \in V, u \in U$:
$\Gamma(g(\alpha \times v))(u) = \Gamma(g\alpha \otimes gv)(u) = A_{g\alpha,gv}(u) = (g\alpha)(u) \cdot gv = \alpha(g^{-1}u) \cdot gv$
$(g\Gamma(\alpha \times v))(u) = (g.A_{\alpha,v})(u) = g \cdot (A_{\alpha,v}(g^{-1}u)) = \alpha(g^{-1}u)gv$ □

5.2.12 Satz: Seien $U, V \in {}_{KG}\mathrm{mod}, |G| = n < \infty$ und sei $\mathrm{char}\, K = p$ mit $p \nmid n$, oder sei $\mathrm{char}\, K = 0$. Dann ist $|G| \cdot 1_K \neq 0$, d.h. $\frac{1}{|G|} = (|G| \cdot 1_K)^{-1}$ existiert in K.
Sei $f : U \to V$ K-linear. Definiere $\hat{f}_G : U \to V : u \mapsto \frac{1}{|G|}\sum_{g\in G} gf(g^{-1}u)$; $\hat{f}_G$ ist KG-linear.
$\hat{f}_G = Tr_(1)^G(f)$ „Spur“.
Beweis: $\hat{f}_G$ ist wohldefinierte Abbildung von $U \to V$. $\hat{f}_G(u_1+u_2) = \frac{1}{|G|}\sum gf(g^{-1}(u_1+u_2)) = \frac{1}{|G|}\sum gf(g^{-1}u_1) + \frac{1}{|G|}\sum gf(g^{-1}u_2) = \hat{f}_G(u_1) + \hat{f}_G(u_2)$.$\hat{f}_G(\lambda u) = \lambda\hat{f}_G(u)$ analog.
Also ist $\hat{f}_G \in \mathrm{Hom}_K(U,V)$.
Sei $h \in G$, dann ist $(h\hat{f}_G)(u) = h \cdot \hat{f}_G(h^{-1}(u)) = \frac{1}{|G|}h(\sum_g gf(g^{-1}(h^{-1}u))) = \frac{1}{|G|}\sum_g (hg)f((hg)^{-1}u) = \frac{1}{|G|}\sum_g gf(g^{-1}u) = \hat{f}_G(u)$.
Also ist $h.\hat{f}_G = \hat{f}_G$, d.h. $\hat{f}_G \in \mathrm{Hom}_K(U,V)^G = \mathrm{Hom}_{KG}(U,V)$. □

5.2.13 Satz (Maschke): Sei G endliche Gruppe, $\mathrm{char}\, K = p \geq 0$. Sei p kein Teiler von $|G|$. Sei $U \in {}_{KG}\mathrm{mod}$ und $V \leq U$. Dann ist V direkter Summand von U, d.h. $\exists W \leq U : V \cap W = (0), V + W = U$.
Beweis: LAAG $\Rightarrow \exists \tilde{W} = K$-Unterraum von U mit $V + \tilde{W} = U$. Sei $\tilde{\pi}$ die natürliche Projektion von U auf V entlang $\tilde{W}$, d.h. $u \in U \Rightarrow \exists! v \in V, \exists! w \in \tilde{W} : u = v + w \Rightarrow \tilde{\pi}(u) = v$.
$\Rightarrow \tilde{\pi}_{|V} = \mathrm{id}_V, \tilde{\pi}_{|\tilde{W}} = 0$.
Nach 5.2.12 ist $\pi = Tr_1^G(\tilde{\pi})$ KG-linear, $\pi(u) = \frac{1}{|G|}\sum_{g\in G} g\tilde{\pi}(g^{-1}u)$.
Sei $v \in V \leq U$. Dann ist $\pi(v) = \frac{1}{|G|}\sum_g g\tilde{\pi}(g^{-1}v) = \frac{1}{|G|}\sum_g gg^{-1}v = \frac{1}{|G|}\sum_g v = v$.
$\Rightarrow U = V \oplus \ker \pi$

5.4.16 Theorem: Sei Δ Divisionsalgebra, $n \in \mathbb{N}$. Dann ist Δ^n (bis auf Isomorphie) der einzige einfache A-Modul, $A = M_{n\times n}(\Delta)$.
Es gilt: ${}_AA = \bigoplus_{n \text{ Kopien}} \Delta^n$
Beweis: Sei $0 \neq x = (\alpha_1, \dots, \alpha_n)^t \in \Delta^n \Rightarrow \exists 1 \leq i \leq n : \alpha_i \neq 0$.
$\alpha_i^{-1} E_{ii} x = e_i \in \xi_n =$ natürliche Basis von Δ^n
$\Rightarrow E_{ji} e_i = e_j$, also $e_j \in A \cdot x \forall 1 \leq j \leq n \Rightarrow \Delta^n = A \cdot x$.
Also ist Δ^n einfach.
Sei für $1 \leq i \leq n$ S_i die Menge der Matrizen aus A, die 0 sind bis auf die i. Spalte.
Dann ist $S_i \leq {}_AA$.
$S_i E_{ij} = S_j$. $\varphi_{E_{ij}} =$ Rechtsmodul mit E_{ij} ist A-Modul Isomorphismus von S_i auf S_j.
$S_i \cong \Delta^n$. Also ist ${}_AA \cong S_1 \oplus \ldots \oplus S_n \cong \bigoplus_{n \text{ Kopien}} \Delta^n$.

Definition: Eine K-Algebra A heißt einfach („simple“), falls (0) und A die einzigen Ideale von A sind.

5.4.17 Lemma: Einfache Algebren sind halbeinfach (semisimple).
Beweis: Sei A eine einfache Algebra, $\Sigma =$ Summe aller einfachen Untermoduln von ${}_AA$.
Klar: Σ ist Linksideal von A. Sei S einfacher Untermodul von ${}_AA$, und sei $a \in A$.
$\rho_a : S \to A : s \mapsto sa$ ist A-Modulhomomorphismu, und daher ist $S \cdot a = \operatorname{im} \rho_a = (0)$ oder $S \cdot a =$ einfacher A-Modul.
In beiden Fällen haben wir $Sa \subseteq \Sigma$, daher ist Σ auch Rechtsideal von A, also ist Σ Ideal von A.
${}_AA$ hat einfache Untermoduln ($\leq (0)$), daher ist $\Sigma \leq (0)$. Da A einfach ist, ist $\Sigma = A$ und daher A semisimple wegen Lemma 5.4.2 (Charakterisierung vo „ss“) und 5.4.13 (Algebra ss. $\Leftrightarrow$ ${}_AA$ ss.). $\square$

5.4.18 Theorem: Sei Δ Divisionsalgebra und sei $n \in N$. Dann ist $A = M_{n\times n}(\Delta)$ einfache Algebra.
Beweis: Sei $(0) \neq J \trianglelefteq A$. Sei $0 \neq a \in J \Rightarrow \exists \alpha_{ij} \in \Delta : a = \sum \alpha_{ij} E_{ij} (1 \leq i, j \leq n)$.
$\exists 1 \leq r, s \leq n : \alpha_{rs} \neq 0$. Sei $1 \leq l, k \leq n$. Dann ist $J \ni b = \alpha_{rs}^{-1} E_{lr} a E_{sk} = \sum \alpha_{rs}^{-1} E_{lr} \alpha_{ij} E_{ij} E_{sk} = \sum \alpha_{rs}^{-1} \alpha_{ij} E_{lr} E_{ij} E_{sk} = \alpha_{rs}^{-1} \alpha_{rs} E_{lk} = E_{lk}$
$\Rightarrow E_{lk} \in J \forall 1 \leq l, k \leq n \Rightarrow J = A$. $\square$

$B_1, \dots, B_r =$ Algebren
$B = B_1 \oplus B_2 \oplus \ldots \oplus B_r$ „ringdirekte“ Summe, d.h. als Λ-Modul ist Summe direkt mit Multiplikation komponentenweise.
$\tilde{B}_i = \{(b_1, \dots, b_r) \mid b_j \in B_j, b_j = 0 \text{ für } j \neq i\} \Rightarrow \tilde{B}_i \cong B_i$ als Λ-Algebra.
$\tilde{B}_i \trianglelefteq B, b_1 \in \tilde{B}_i, b_2 \in \sum_{i\neq j} \tilde{B}_j \Rightarrow b_1 b_2 = b_2 b_1 = 0$
$\tilde{B}_i \cap \tilde{B}_j = (0) \quad (i \neq j)$.
$\tilde{B}_i$ heißen „Blöcke“ von B (Blockideale).

5.4.19 Lemma: $B = B_1 \oplus \ldots \oplus B_r$ ringdirekte Summe von Algebren B_i. Dann sind die

zweiseitigen Ideale von B genau die Mengen der Form $J = J_1 \oplus \ldots \oplus J_r$ mit $J_i \trianglelefteq B_i$ $(J_i = J \cap \tilde{B}_i)$.
Beweis: Setze $J_i = J \cap B_i \trianglelefteq B$. Klar: $\sum\limits_{i=1}^{r} J_i = \bigoplus\limits_{i=1}^{r} JJ - i \subseteq J$. Sei $b \in J, b = b_1 + \ldots b_r$ mit $b_i \in B_i$ und $1 = e_1 + \ldots + e_r, e_j = 1_{B_j}$.
Dann ist $bcdote_1 = b_1e_1 + b_2e_1 + \ldots + b_re_r = b_1 \in J_1$, analog $b_i \in B_i \Rightarrow$ Behauptung.

5.4.20 Theorem: Sei $r \in \mathbb{N}, \Delta_i$ Divisionsalgebra über K endlicher Dimension, $n_i \in N, B_i = M_{n_i \times n_i}(\Delta_i) \forall 1 \leq i \leq r$.
Sei $B = B_1 \oplus \ldots \oplus B_r$ ringdirekte Summe. $(\dim_K B = \sum_{i=1}^{r} \dim_K(\Delta_i) n_i^2 < \infty)$. Dann ist B semisimple, und es gibt exakt r viele nicht isomorphe einfache B-Moduln, und gneau 2^4 zweiseitige Ideale von B, nämlich $\bigoplus_{j \in J} B_j$ mit $J \subseteq \{1, \ldots, r\}$ (Ideale), einfachen B-Moduln $S_1, \ldots, S_r$ mit $S_i \leq \ _{B_i}B_i$ einfach.
Beweis: Ist $S \leq \ _{B_i}B_i$ einfacher Untermodul, so ist auch S ein einfacher B-Modul mit $b \cdot x = 0 \forall b \in B_j$ mit $j \neq i$. $(U \leq \ _{B_i}B_i \leq_{\text{Liid}} \ _BB$ immer).
Haben gesehen (5.4.16): $\forall 1 \leq i \leq r$ gibt es genau einen einfachen B_i-Modul S_i, $B_i \cong \bigoplus\limits_{n_i \text{ Kopien}} S_i. \Rightarrow \ _BB \cong \bigoplus\limits_{i=1}^{r} \bigoplus\limits_{n_i \text{ Kopien}} S_i$.
Insbesondere ist $_BB$ (direkte) Summe einfacher Untermoduln, und daher nach 5.4.13 semisimple. Jeder einfache B-Modul ist daher isomorph zu einem S_i mit $1 \leq i \leq r$ (5.4.14).
Behauptung folgt sofort aus 5.4.18 und 5.4.19. $\square$

5.4.21 Satz: Sei $0 \neq e^2 = e \in B \Rightarrow \mathrm{End}_B(Be) \cong eBe$.

5.4.22 Lemma:Sei B Algebra. Dann ist $M_{n\times n}(B)^{op} \cong M_{n \times n}(B^{op})$.
Beweis Idee: $M_{n\times n}(B)^{op} \to M_{n\times n}(B^{op}) : a \mapsto a^t$ ist Isomorphismus.

5.4.23 Theorem (Wedderburn): Eine K-Algebra A $(\dim_K A < \infty)$ ist semisimple $\Leftrightarrow A = \bigoplus\limits_{i=1}^{r} M_{n_i \times n_i}(\Delta_i)$ mit $\Delta_i =$ Divisionsalgebra über K mit $\dim_K \Delta_i < \infty$.
Beweis: „$\Leftarrow$“ ist 5.4.20.
Sei also A semisimple. Sei $S_1, \ldots, S_r$ eine vollständige Menge paarweiser nicht isomorpher einfacher A-Moduln und sei $\Delta_i = \mathrm{End}_A(S_i)$ Schiefkörper $(\dim_K \Lambda_i = k)$, $n_i = \dim_{\Delta_i}(S_i)$
Da $_AA$ semisimple gibt es $v_1, \ldots, v_r \in \mathbb{N} : \ _AA = S_1^{\oplus v_1} \oplus \ldots \oplus S_r^{\oplus v_r}$.
$5.4.21 \Rightarrow \mathrm{End}_A(\ _AA) = 1 \cdot A \cdot 1 \cong A$
$\mathrm{End}_A(S_1^{\oplus v_1} \oplus \ldots \oplus S_r \oplus v_r) \cong_{\text{Satz 5.4.12}} M_{v_1 \times v_1}(\Delta_1) \oplus \ldots \oplus M_{v_r \times v_r}(\Delta_r)$
$5.4.20 \Rightarrow v_i = n_i$ $\square$.

5.4.25 Spezialfall: A semisimple K-Algebra, K algebraisch abgeschlossen. Dann $\exists n_1, \ldots, n_r \in \mathbb{N} : A \cong M_{n_1 \times n_1}(K) \oplus \ldots M_{n_r \times n_r}(K)$
$\{S_1, \ldots, S_r\} =$ vollständige Menge nicht isomorpher einfacher A-Moduln, $\dim_K S_i = n_i$.

VI. Charaktere

$G =$ endliche Gruppe, alle $\mathbb{C}G$-Moduln sind endlich erzeugt.

6.1.1 Anmerkung: $G =$ endliche Gruppe $\Rightarrow^{\text{Maschke}} \mathbb{C}G$ ist semisimple.
$\Rightarrow \exists n_i \in \mathbb{N} : \mathbb{C}G \cong M_{n_1 \times n_1}(\mathbb{C}) \oplus \ldots M_{n_r \times n_r}(\mathbb{C})$ 6.1.2 : $\sum n_i^2 = |G|$

Bemerkung: char $K \nmid |G| \Rightarrow KG$ semisimple. $KG \cong M_{n_1 \times n_1}(\Lambda_1) \oplus \ldots \oplus M_{n_r \times n_r}(\Lambda_r)$
Fakten: 1) Λ_i kommutativ
2) $K = \mathbb{C} : n_i$ Teiler von $|G|$

6.1.3 Theorem: $|\{$einfache $\mathbb{C}G$-Moduln$\}| = |\{$Konjugationsklassen von $G\}| = \dim_{\mathbb{C}} Z(\mathbb{C}G)$
Beweis: $\mathbb{C}G = M_{n_1 \times n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_r \times n_r}(\mathbb{C}) \exists r, n_1, \ldots, n_r \in \mathbb{N}$ (6.1.1)
$\Rightarrow_{5.4.23}$ Anzahl nicht isomorpher irreduzibler $\mathbb{C}G$-Moduln $= r$
Klar: $B = B_1 \oplus \ldots \oplus B_r$ ringdirekte Summe $\Rightarrow Z(B) = Z(B_1) \oplus \ldots \oplus Z(B_r)$
$Z(M_{n \times n}(\mathbb{C})) = \{\alpha 1_M \mid \alpha \in \mathbb{C}\}$. Also ist $\dim_K(Z(\mathbb{C}G)) = r$.
Sei $x = \sum \alpha_g g$ mit $\alpha_g \in \mathbb{C}$
$x \in Z(\mathbb{C}G) \Leftrightarrow hx = xh \forall h \in G \Leftrightarrow x = hxh^{-1} \forall h \in G$
d.h. $x \in Z(\mathbb{C}G) \Leftrightarrow \sum \alpha_g g = \sum \alpha_g hgh^{-1} \forall h \in G$
$\sum \alpha_g g = \sum \alpha_{hgh^{-1}} g \Rightarrow \forall h \in G : \alpha_{hgh^{-1}} = \alpha_g$.
Sei $C_1, \ldots, C_m$ Konjugationsklassen von G, $g_i \in C_i, \hat{C}_i = \sum_{h \in C_i} h$.
$\Rightarrow x = \sum_{i=1}^m \alpha_g \hat{C}_i$.
Klar: $(\hat{C}_1, \ldots, \hat{C}_m) \subseteq \mathbb{C}G$ lineare unabhängig/$\mathbb{C}$.
$\Rightarrow (\hat{C}_1, \ldots, \hat{C}_m)$ ist $\mathbb{C}$-Basis von $Z(\mathbb{C}G) \Rightarrow \dim_{\mathbb{C}}(Z(\mathbb{C}G)) = m =$ Anzahl der Konjugationsklassen $= r =$ Anzahl der irreduziblen $\mathbb{C}G$-Moduln.

$G =$ endliche Gruppe, $\mathbb{C}G$, $M \in {}_{\mathbb{C}G}\text{mod}$, zugehörige Darstellung $\varphi : \mathbb{C}G \to \operatorname{End}_{\mathbb{C}}(M)$

Definition: Sei $\varphi : \mathbb{C}G \to \operatorname{End}_{\mathbb{C}}(M)$ Darstellung, $\dim_{\mathbb{C}} M < \infty$. Dann heißt die Abbildung $\chi_M = \chi_\varphi : G \to \mathbb{C} : g \mapsto \operatorname{tr}(\varphi(g))$ („gewöhnlicher“) Charakter zur Darstellung φ.

Beachte: $\varphi(g) \in \operatorname{End}_{\mathbb{C}}(M) \cong M_{n \times n}(\mathbb{C})$
$\operatorname{tr}(m_f(\mathcal{B}, \mathcal{B}))$ ist unabhängig von der Wahl von $\mathcal{B}$, da $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, also $\operatorname{tr}(PAP^{-1}) = \operatorname{tr}(AP^{-1}P) = \operatorname{tr}(A)$.

Also ist die Spur $\mathrm{tr}(f)$ für $f \in \mathrm{End}_{\mathbb{C}}(M)$ wohldefiniert, wenn wir $\mathrm{tr}(f) := \mathrm{tr}(m_f(\mathcal{B},\mathcal{B}))$ setzen für irgendeine $\mathbb{C}$-Basis von M.

Klar: Ist $M \cong N, M, N \in {}_{\mathbb{C}G}\mathrm{mod}$, so ist $\chi_M = \chi_N$.
Seien $\varphi : G \to \mathrm{Aut}_{\mathbb{C}}(M) \to \mathrm{GL}_m(\mathbb{C})(\dim_{\mathbb{C}} M = m)$
und $\psi : G \to \mathrm{Aut}_{\mathbb{C}}(N) \to \mathrm{GL}_n(\mathbb{C})(\dim_{\mathbb{C}} N = n)$
Erinnerung: Sei $\tau : M \to N$ $\mathbb{C}G$-Isomorphismus. Dann gilt: $m = n$ und $\forall g \in G$:

$$\begin{array}{ccc} M & \xrightarrow{\varphi(g)} & M \\ \tau\downarrow & & \tau\downarrow \\ N & \xrightarrow{\psi(g)} & N \end{array} \qquad \begin{array}{ccc} \mathbb{C}^n & \xrightarrow{\tilde{\varphi}(g)} & \mathbb{C}^n \\ \tau\downarrow & & \tau\downarrow \\ \mathbb{C}^n & \xrightarrow{\tilde{\psi}(g)} & \mathbb{C}^n \end{array}$$

$\tau\tilde{\varphi}(g) = \tilde{\psi}(g)\tau \Leftrightarrow \tilde{\varphi}(g) = \tau^{-1}\tilde{\psi}(g)\tau$
$\Rightarrow \chi_M(g) = \mathrm{tr}(\tilde{\varphi}(g)) = \mathrm{tr}(\tilde{\psi}(g))\forall g \in G$

Beispiel:

i) Sei $M = \mathbb{C}_G$ triviale $\mathbb{C}G$-Modul, d.h. $(\sum \lambda_g g)z = (\sum \lambda_g)z, \quad (\lambda_g, z \in \mathbb{C})$
$\chi_M : g \to 1 \in \mathbb{C}$

ii) Sei Ω eine transitive G-Menge, $M_\Omega =$ zugehöriger $\mathbb{C}G$-Modul.
Ohne Einschränkung $\Omega = \{1, \ldots, n\}$, $G \hookrightarrow \sigma_n \cong W \leq GL_n(\mathbb{C})$
Sei $P_\pi =$ Permutationsmaatrix zu $\pi \in \sigma_n, \mathrm{tr}(P_\pi) = |\{i \in \{1, \ldots, n\} \mid \pi(i) = i\}|$.
$\mathrm{tr}(g) = |\{w \in \Omega \mid gw = w\}|$

Spezialfall: $M = {}_{\mathbb{C}G}\mathbb{C}G$.
Sei χ_M zugehöriger Charakter.
$\chi_M(g) = |\{x \in G \mid gx = x\}| = \begin{cases} 0 & \text{für } g \neq 1 \\ |G| & \text{für } g = 1 \end{cases}$

iii) Sei $\chi : G \to \mathbb{C}$ Charakter zum $\mathbb{C}G$-Modul M.
$\chi(1) = \dim_{\mathbb{C}} M$.

Bezeichnung: Seien $S_1, S_2, \ldots, S_r$ die verschiedenen irreduziblen $\mathbb{C}G$-Moduln, wobei S_1 der triviale $\mathbb{C}G$-Modul ist. Wir bezeichnen den Charakter χ_{S_i} des i-ten $\mathbb{C}G$-Modules mit $\chi_i(i = 1, \ldots, r)$
$\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$.
Die χ_i heißen irreduzible Charaktere.
Sei $f_i = \dim_{\mathbb{C}} S_i : \mathbb{C}G = \bigoplus_{i=1}^{r} M_{f_i \times f_i}(\mathbb{C})$

Bemerkung: Ist $\dim_{\mathbb{C}} M = 1$ (z.Bsp. S_1), so spricht man von einem linearen Charakter, denn $\chi_M : G \to \mathbb{C}^*$ ist Gruppenhomomorphismus.

6.1.4 Satz: Sei $U \in {}_{\mathbb{C}G}\mathrm{mod}, \rho : G \to \mathrm{GL}_{\mathbb{C}}(U) \subseteq \mathrm{End}_{\mathbb{C}}(U)$ zugehörige Darstellung. Sei $g \in G, |g| = n$.
Dann gilt:

i) $\rho(g) \in \mathrm{End}_{\mathbb{C}}(U)$ ist diagonalisierbar

ii) $\chi_U(g)$ = Summe (mit Vielfachheiten) der Eigenwerte von $\rho(g)$ (LAAG 2: Jordansche NF)

iii) $\chi_U(g)$ = Summe von $\chi_U(1) = \dim_{\mathbb{C}} U$ vielen n-ten Einheitswurzeln.

iv) $\chi_U(g^{-1}) = \overline{\chi_U(g)}$

v) $|\chi_U(g)| = \sqrt{\chi_U(g)\overline{\chi_U(g)}} \leq \chi_U(1)$

vi) $\{g \in G \mid \chi_U(x) = \chi_U(1) = \dim_{\mathbb{C}} U\} \trianglelefteq G$.

Beweis:

i) $g^n = 1 \Rightarrow (\rho(g))^n = \mathrm{id}_U \rightsquigarrow E_{\dim_{\mathbb{C}}(U)} \Rightarrow \rho(g)$ genügt dem Polynom $x^n - 1 \in \mathbb{C}[X] \Rightarrow$ Minimalpolynom $\mu_{\rho(g)}(t)$ hat nur einfache Nullstellen $\Rightarrow \rho(g)$ ist diagonalisierbar.

ii) Folgt aus i)

iii) Folgt aus i)

iv) Jeder Eigenvektor von $\rho(g)$ zu einem Eigenwert $z \in \mathbb{C}$ ist Eigenvektor von $\rho(g^{-1})$ zum Eigenwert $z^{-1} \in \mathbb{C}$:
$\rho(g)v = zv \Rightarrow z^{-1}v = (\rho(g)^{-1})(v) = \rho(g^{-1})(v), z\overline{z} = |z|^2 = 1^2 = 1 \Rightarrow \overline{z} = z^{-1}$
$\chi_\rho(g) = \sum$ Einheitswurzeln, $\chi_{\rho^{-1}} = \sum \overline{\text{Einheitswurzeln}} = \overline{\sum \text{Einheitswurzeln}} = \overline{\chi_U(g)}$
$|\chi_U(g)| = |\sum_{\dim_{\mathbb{C}} U} \text{Eigenwerte } h| \overset{\text{Dreiecks-Ugl.}}{\leq} \sum_{\dim_{\mathbb{C}}(U)} |\text{Eigenwert h}| = \dim_{\mathbb{C}} U = \chi_U(1)$.

vi) $|z_1 + z_2| = |z_1| + |z_2| \Leftrightarrow z_1 = \lambda z_2 \exists \lambda \in \mathbb{R}^+$

v) $\Rightarrow |\chi_U(g)| = \chi_U(1) \Leftrightarrow$ ale Eigenwerte von $\rho(g)$ sind 1 $\Leftrightarrow \rho(g) = \mathrm{id}_U \Leftrightarrow g \in \ker \rho_U \trianglelefteq G$.
$\rho_U : G\,\mathrm{Aut}_{\mathbb{C}}(U)$

Erinnerung: $\mathbb{C}^G = \{\alpha : G \to \mathbb{C}\}$ ist $\mathbb{C}$-Algebra mit Addition $(\alpha_1 + \alpha_g)(g) = \alpha_1(g) + \alpha_2(g), (\alpha_1 \cdot \alpha_2)(g) = \alpha_1(g) \cdot \alpha_2(g)$ und $(\lambda\alpha)(g) = \lambda(\alpha(g))$.
Menge Der Charaktere von $G \subseteq \mathbb{C}^G$.

6.1.5 Lemma: $(\chi_1, \ldots, \chi_r)$ ist linear unabhängig in dem $\mathbb{C}$-Vektorraum $\mathbb{C}^G$.

Beweis: $\mathbb{C}G \cong M_{f_1\times f_1}(\mathbb{C}) \oplus \ldots \oplus M_{f_r\times f_r}(\mathbb{C})$, S_i = der eindeutig bestimmte irreduzible G-Modul im Block $M_{f_i\times f_i}(\mathbb{C})$.
Sei e_i = Einselement von $M_{f_i\times f_i}(\mathbb{C})$ (also $e_i = ((0)_{f_1\times f_1}, \ldots, (0)_{f_{i-1}\times f_{i-1}}, (1)_{f_i\times f_i}, (0)\ldots))$ Idemp. von $\mathbb{C}G$.
Seien $\chi_1, \ldots, \chi_r$ die zu S_i gehörenden Charaktere von G.
Wir können χ_i linear zu einer lineare Abbildung vn $\mathbb{C}G$ nach $\mathbb{C}$ ausdehnen: $\chi_i \in \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}G, \mathbb{C}) = \mathbb{C}G^*$, d.h.für $a = \sum\limits_{g\in G} \alpha_g g \in \mathbb{C}G$ ist $\chi_i(\alpha) = \sum\limits_{g\in G} \alpha_g \chi_i(g) \in \mathbb{C}$.
Beachte: Auf S_i operiert e_i wie die Eins. D.h. $\chi_i(e_i) = \dim_{\mathbb{C}}(S_i) = f_i$ und $\chi_j(e_i) = 0$ für $i \neq j$.
Seien $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ so, dass $\sum\limits_{j=1}^{r} \lambda_j\chi_j = 0$ ist. Dann ist für $1 \leq i \leq r : 0 = \sum\limits_{j=1}^{r} \lambda_j\chi_j)(e_i) = \lambda_i\chi_i(e_i) \Rightarrow \lambda_i = 0 \forall i$. Also sind $(\chi_1, \ldots, \chi_r)$ linear unabhängig.

6.1.6 Lemma: $U, V \in {}_{\mathbb{C}G}\mathrm{mod}$ endlich erzeugt. Dann $\chi_{U\oplus V} = \chi_U + \chi_V$
Beweis: Trivial. ($\rho_{U\oplus V}(g)$ hat Blockdiagonalform. Spur nehmen $\Rightarrow$ Behauptung.)

Beachte: Sind $g, h \in G$ konjugiert, χ Charakter von $G \Rightarrow \chi(g) = \chi(u)$, denn g, h konjugiert $\Rightarrow \exists x \in G : g = xhx^{-1} \Rightarrow \chi(g) = \chi(xhx^{-1}) = \chi((hx^{-1})x) = \chi(h)$, d.h. χ ist konstant auf Konjugationsklassen von G.
Abbildung $\alpha : G \to \mathbb{C}(\alpha \in \mathbb{C}^G)$ heißen <u>Klassenfunktionen</u>, wenn $\alpha(g) = \alpha(h)$ falls g, h konjugiert sind.

Wir haben gezeigt: $\chi_1, \ldots, \chi_r$ sind r viele linear unabhängig Klassenfunktionen in $\mathbb{C}^G$.
Definiere: $C_1, \ldots, C_r$ seien die Konjugationsklassen auf G. Für $1 \leq i \leq r$ sei $\epsilon_i : g \mapsto \begin{cases} 1 & \text{falls } g \in C_i \\ 0 & \text{sonst} \end{cases}$
Klar: $\{\epsilon_1, \ldots, \epsilon_r\}$ linear unabhängig in der Unteralgebra der Klassenfunktionen.
Sei $\alpha : G \to \mathbb{C}$ Klassenfunktion, mit $\alpha(g) = \alpha_i \in \mathbb{C}$ für $g \in C_i \Rightarrow \alpha = \alpha_1\epsilon_i + \ldots + \alpha_r\epsilon_r$

Folgerung: $\{\chi_1, \ldots, \chi_r\}$ ist Basis der $\mathbb{C}$-Algebra der Klassenfunktionen auf G.

Bemerkung: Sei $M \in {}_{\mathbb{C}G}\mathrm{mod}$ endlich erzeugt $\Rightarrow \exists \nu_1, \ldots, \nu_r \in \mathbb{N}_0$ so, dass $M = S_1^{\oplus\nu_1} \oplus \ldots \oplus S_r^{\oplus\nu_r} \Rightarrow \chi_M = \nu_1\chi_1 + \ldots + \nu_r\chi_r$.

Es gilt: Ist $M \ncong N$ und $M, N \in {}_{\mathbb{C}G}\mathrm{mod}$ endlich erzeugt $\Rightarrow \chi_M \neq \chi_N$.

6.1.7 Satz: Zwei endliche erzeugte $\mathbb{C}G$-Moduln sind isomorph $\Leftrightarrow$ ihre Charakter stimmen überein.
Beweis: Sind $S_1, \ldots, S_r$ die verschiedenen irreduziblen $\mathbb{C}G$-Moduln mit Charakteren $\chi_1, \ldots, \chi_r, M, N \in {}_{\mathbb{C}G}\mathrm{mod}$. Sei $M = S_1^{\oplus\mu_1} \oplus \ldots \oplus S_r^{\oplus\mu_r}, N = S_1^{\oplus\nu_1} \oplus \ldots \oplus S_r^{\oplus\nu_r}$, so ist $\chi_M = \sum\limits_{i=1}^{r} \mu_i\chi_i, \chi_N = \sum\limits_{i=1}^{r} \nu_i\chi_i$
$M \cong N \Leftrightarrow \mu_i = \nu_i \forall i = 1, \ldots, r \Leftrightarrow \chi_M = \chi_N$ $\square$

Bemerkung: Es gibt keinen kanonischen Weg, aus dem Charakter eines $\mathbb{C}G$-Moduls M den Modul M selbst zu bestimmen.

Erinnerung: $U, V \in {}_{\mathbb{C}G}\text{mod} \Rightarrow U \otimes_{\mathbb{C}} V, \text{Hom}_{\mathbb{C}}(U,V), U^* = \text{Hom}_{\mathbb{C}}(U, \mathbb{C})$ sind $\mathbb{C}G$-Moduln.

6.1.8 Satz: $U, V \in {}_{\mathbb{C}G}\text{mod}$. Dann gilt:

i) $\chi_{U \times V} = \chi_U \cdot \chi_V (\chi_{U \otimes V}(g) = \chi_U(g) \cdot \chi_V(g))$

ii) $\chi_{U^*} = \overline{\chi_U} (\chi_{U^*}(g) = \overline{\chi_U(g)}$

iii) $\chi_{\text{Hom}_{\mathbb{C}}(U,V)} = \overline{\chi_U} \cdot \chi_V$

Beweis:

i) Sei $g \in G$. Sei $(u_1, \ldots, u_m)$ und $(v_1, \ldots, v_n)$ Basen von U bzw. V aus Eigenvektoren von g auf U bzw. V. D.h. $\exists \mu_1, \ldots, \mu_m, \nu_1, \ldots, \nu_n \in \mathbb{C} : gu_i = \mu_i u_i$ und $gv_j = \nu_j v_j \forall 1 \leq i \leq m, 1 \leq j \leq n$.
Dies geht nach 6.1.4, da die Operation von G auf U bzw. V diagonalisierbar ist.
LAAG: Die $(u_i \otimes v_j \mid 1 \leq i \leq m, 1 \leq j \leq n)$ ist Basis von $U \otimes V$
$g(u_i \otimes v_i) = (gu_i) \otimes (gv_j) = (\mu_i u_i) \otimes (\nu_j v_j) = \mu_i \nu_j (u_i \otimes v_j)$
Es folgt: $\chi_{U \otimes V}(g) = \sum\limits_{i,j} \mu_i \nu_j = (\sum\limits_{i=1}^{m} \mu_i)(\sum\limits_{j=1}^{n} \nu_j) = \chi_U(g) \chi_V(g)$

ii) $g \in G, (u_1, \ldots, u_m)$ Basis aus Eigenvektoren von g auf U, $gu_i = \mu_i u_i, \mu_i \in \mathbb{C}, 1 \leq i \leq m$.
Sei $(u_1^*, \ldots, u_m^*)$ Basis von U^*, d.h. $u_i^*(u_j) = \delta_{ij}$. $\Rightarrow (gu_i^*)(u_j) = u_i^*(g^{-1}u_j) \overset{6.1.4}{=} u_i^*(\mu_j u_j) = \overline{\mu_j} \delta_{ij}$
$\Rightarrow gu_i^* = \overline{\mu_i} u_i^*$, d.h. u_i^* ist Eigenvektor von Operation von g auf U^* mit Eigenwerten $\overline{\mu_i}$.
Also ist $\chi_{U^*}(g) = \sum\limits_{i=1}^{m} \overline{\mu_i} = \overline{\sum\limits_{i=1}^{m} \mu_i} = \overline{\chi_U(g)}$.

iii) Nach 5.3.4 (?) ist $\text{Hom}_{\mathbb{C}}(U, V) \cong U^* \otimes V$ als $\mathbb{C}G$-Modul. Die Behauptung folgt aus i) und ii). $\square$

Bemerkung: $\{\text{char von } G\} \subseteq \mathbb{C}^G = \mathbb{C}$-Algebra und darin sind die irreduziblen Charaketere $(\chi_1, \ldots, \chi_r)$ linear unabhängig. So ist $< \chi_1, \ldots, \chi_r >_{\mathbb{C}\text{-Aufspann}}$ r-dimensionaler Unterraum von $\mathbb{C}^G$.
Abelsche Gruppe, freier $\mathbb{Z}$-Modul: $\left\{ \sum\limits_{i=1}^{r} \mu_i \chi_i \mid \mu_i \in \mathbb{Z} \right\} \subseteq < \chi_1, \ldots, \chi_r >$.
Klassenfunktionen der Form $\sum\limits_{i=1}^{r} \mu_i \chi_i$ mit $\mu_i \in \mathbb{Z}$ heißen „virtuelle“ Charaktere.

6.1.9 Korrolar: Der Raum der virtuellen Charaktere ist ein Ring.

Beweis: Nach 6.1.8 ist das Produkt zweier Charaktere wieder ein Charakter, d.h. ganzzahlige Linearkombination der $\chi_1, \ldots, \chi_r$. Also ist auch das Produkt zweier virtueller Charaktere wieder ein virtueller Charakter. $\square$

Definition: Eine Klassenfunktion auf G ist eine Abbildung $f : G \to \mathbb{C}$ mit $f(g) = f(h)$ falls g, h konjugiert (also $g \sim_G h$).
Klar: Summe, lineare Vielfache und Produkte vo Klassenfunktionen sind Klassenfunktionen.
Also: $< \chi_1, \ldots, \chi_r >_{\mathbb{C}} \subseteq \{\text{Klassenfunktionen auf } G\} \leq \mathbb{C}^G$

6.1.10 $< \chi_1, \ldots, \chi_r >_{\mathbb{C}}$ ist die $\mathbb{C}$-Algebra der Klassenfunktionen.auf G.
Beweis: Seien $C_1, \ldots, C_r$ die Konjugationsklassen von G, $1 \leq i, j \leq r$. Sei $\psi_i : G \to \mathbb{C}$ definiert durch:
$\psi_i(g) = \begin{cases} 1 & \text{für } g \in C_i \\ 0 & \text{sonst} \end{cases}$
Sei $f : G \to \mathbb{C}$ Klassenfunktion mit $f(g) = \lambda_i$ für $g \in C_i \Rightarrow f = \sum\limits_{i=1}^{r} \lambda_i \psi_i \Rightarrow f \in < \psi_1, \ldots, \psi_r >_{\mathbb{C}}$
Trivial: $\psi_1, \ldots, \psi_r$ linear unabhängig $\Rightarrow \dim_{\mathbb{C}} \{\text{Klassenfunktionen auf } \mathbb{C}\} = r$
$\Rightarrow$ Behauptung. $\square$

Definition: $\mathrm{Cl}(G) :=$ $\mathbb{C}$-Vektorraum der Klassenfunktionen auf G.
Auf $\mathrm{Cl}(G)$ definieren wir ein inneres Produkt $(\cdot, \cdot)$ durch: $(\alpha, \beta \in \mathrm{Cl}(G))$
$(\alpha, \beta) = \frac{1}{|G|} \sum\limits_{g \in G} \alpha(g)\overline{\beta(g)} \in \mathbb{C}$
Wir haben:

$$(\alpha, \alpha) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\alpha(g)} = \frac{1}{|G|} \sum_{g \in G} |\alpha(g)|^2 = 0 \Leftrightarrow \alpha(g) = 0 \forall g \in G \Leftrightarrow \alpha = 0.$$

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)} = \frac{1}{|G|} \sum_{g \in G} \overline{\beta(g)\overline{\alpha(g)}} = \overline{(\beta, \alpha)}$$

$$(\lambda\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} (\lambda\alpha)(g)\overline{\beta(g)} = \frac{\lambda}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)} = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{(\overline{\lambda}\beta)(g)} = (\alpha, \overline{\lambda}\beta)$$

$$(\alpha_1 + \alpha_2, \beta) = \frac{1}{|G|} \sum_{g \in G} \alpha_1(g)\overline{\beta(g)} + \frac{1}{|G|} \sum_{g \in G} \alpha_2(g)\overline{\beta(g)} = (\alpha_1, \beta) + (\alpha_2, \beta).$$

Also ist $(\cdot, \cdot)$ wirklich ein Skalarprodukt auf Cl()G).

Erinnerung: $U \in {}_{\mathbb{C}G}\underline{\text{mod}}$ endlich erzeugt. Dann ist $U^G = \{u \in U \mid gu = u \forall g \in G\}$ ist der eindeutig bestinmmte größte Untermodul von U, auf dem G trivial operiert.
$U = S_1^{\oplus \mu_1} \oplus \ldots \oplus S_r^{\oplus \mu_r}, S_1 =$ trivialer $\mathbb{C}G$-Modul.
$\Rightarrow U^G = S_1^{\oplus \mu_1}, \mu_1 = \dim_{\mathbb{C}} U^G$

Beobachtung: $U^G =$ simultae Eigenraum $\forall g \in G$ zum Eigenwert $1 = \bigcap\limits_{g \in G}$ Eigenraum von g zum Eigenwert 1.

6.1.11 Lemma: Sei $U \in {}_{\mathbb{C}G}\underline{\text{mod}}$ endlich erzeugt, dann ist $\dim_{\mathbb{C}} U^G = \frac{1}{|G|}\sum_{g\in G}\chi_U(g)(= \chi_U(\frac{1}{|G|}\sum_{g\in G} g = \chi_U(T))$.
Beweis: Sei $a = \frac{1}{|G|}\sum_{g\in G} g \in \mathbb{C}G$. Sei $h \in G \Rightarrow ha = \frac{1}{|G|}\sum_{g\in G} hg = \frac{1}{|G|}\sum_{g\in G} g = a = ah$
$\Rightarrow a^2 = (\frac{1}{|G|}\sum_{g\in G} g)a = \frac{1}{|G|}\sum_{g\in G}(ga) = \frac{1}{|G|}\sum_{g\in G} a = a, a$ ist Idempotent von $\mathbb{C}G$.
$(\mathbb{C}G = M_{1\times 1}(\mathbb{C}) \oplus M_{f_2\times f_2}(\mathbb{C}) \oplus \ldots \oplus M_{f_r\times f_r}(\mathbb{C}); a = (1, 0, \ldots, 0)$.
Sei $\rho : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(U)$ die zu $U \in {}_{\mathbb{C}G}\underline{\text{mod}}$ gehörende Darstellung von ${}^{\mathbb{C}}G$ und sei $T = \rho(a)$.
Dann gilt $T^2 = (\rho(a))^2 = \rho(a^2) = \rho(a) = T$, d.h. T erfüllt das Polynom $X^2 - X \in \mathbb{C}[X] \Rightarrow 0$ und 1 sind die einzigen möglichen Eigenwerte von T und T ist diagonalisierbar.

Sei $U_1 \subseteq U$ der Eigenraum von T zum Eigenwert 1.
$u \in U_1 \Rightarrow g(u) = g(a \cdot u) = (ga)(u) = au = u$
$\Rightarrow U_1 \leq U^G$
Sei $u \in U^G$, dann ist $|G|au = (\sum_{g\in G} g)u = \sum_{g\in G}(gu) = \sum_{g\in G} u = |G|u \Rightarrow au = u \Rightarrow u \in U_1$
Also ist $U_1 = U^G$. Die Spur $\mathrm{tr}(T)$ von T auf U ist $\dim_{\mathbb{C}}(U_1)$

6.1.12 Erinnerung: Sind $U, V \in {}_{\mathbb{C}G}\underline{\text{mod}}$ endlich erzeugt. Dann ist $\mathrm{Hom}_{\mathbb{C}}(U, V) = U^* \otimes V \in {}_{\mathbb{C}G}\underline{\text{mod}}$ und es ist $\mathrm{Hom}_{\mathbb{C}G}(U, V) = (\mathrm{Hom}_{\mathbb{C}}(U, v))^G$.

6.1.13 Korrolar: Seien $U, v \in {}_{\mathbb{C}G}\underline{\text{mod}}$. Dann ist $(\chi_V, \chi_U) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(U, V)$
Beweis: $\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(U, V) \overset{6.1.12}{=} \dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}}(U, V))^G \overset{6.1.11}{=} = \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}_{\mathbb{C}}(U,V)}(g)$

$\overset{6.1.8}{=} \frac{1}{|G|}\sum_{g\in G}(\overline{\chi_U(g)}\chi_V(g)) = (\chi_V, \chi_U)$ □

Bemerkung: $\mathrm{Hom}_{\mathbb{C}G}(S_1^{\oplus\nu_1} \oplus \ldots \oplus S_r^{\oplus\nu_r}, S_1^{\oplus\mu_r} \oplus \ldots \oplus S_r^{\oplus\mu_r}) = \bigoplus_{i=1}^{r} \mathrm{Hom}_{\mathbb{C}G}(S_i^{\oplus\nu_i}, S_i^{\oplus\mu_i}) \cong M_{\mu_i\times\nu_i}(\mathbb{C})$
$\dim = \sum \mu_i\nu_i$

6.1.14 Korrolar: $\chi_1, \ldots, \chi_r$ ist eine Orthonormalbasis von $\mathrm{Cl}(G)$. Beweis: 6.1.13 impliziert, dass $(\chi_i, \chi_j) = \delta_{ij}$. □.