Algebra Skript
Prof. Pahlings
Wintersemester 2000/2001

Thomas Franken
Thomas.Franken@post.rwth-aachen.de

19. Juli 2001

Inhaltsverzeichnis

I Algebra I **2**

1 Gruppen **3**
1.1 Gruppen und Untergruppen . . . 3
1.2 Operationen von Gruppen auf Mengen . . . 4
1.3 Bahnen . . . 6
1.4 Der Bahnensatz . . . 7
1.5 Konjugiertenklassen . . . 9
1.6 Abzählen von Bahnen . . . 11
1.7 Der verfeinerte Bahnalgorithmus . . . 12
1.8 Normalteiler . . . 13
1.9 Gruppen mit Operatorenbereich . . . 15
1.10 Die Isomorphiesätze . . . 15
1.11 Automorphismen . . . 17
1.12 Zyklische Gruppen und ihre Automorphismen . . . 18
1.13 Direkte Produkte und der chinesischer Restesatz . . . 19
1.14 Die Sylowsätze . . . 20
1.15 Endliche abelsche Gruppen . . . 22
1.16 Kompositionsreihen . . . 23
1.17 Auflösbare Gruppen . . . 24
1.18 Einfache Gruppen . . . 25

2 Ringe **27**
2.1 Ringe und Ideale . . . 27
2.2 Integritätsringe und Quotientenkörper . . . 28
2.3 Hauptideale . . . 30
2.4 Faktorielle Ringe . . . 31
2.5 Polynomringe über faktoriellen Ringen . . . 32
2.6 Faktorisierung von Polynomen . . . 34

3 Körper **36**
3.1 Primkörper und Körpererweiterungen . . . 36
3.2 Algebraische und transzendente Elemente . . . 37

Teil I

Algebra I

Kapitel 1

Gruppen

1. Vorlesung vom 18.10.2000

1.1 Gruppen und Untergruppen

Definition: Sei $G \neq \emptyset$ mit einer Abbildung $\star : G \times G \to G$
dann heißt
a) $(G, \star)$ eine **Halbgruppe** $\Leftrightarrow \forall g_1, g_2, g_3 \in G : (g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$
b) gilt zusätzlich: $\exists \epsilon \in G \; \forall g \in G : \epsilon \star g = g \star \epsilon = g$, so heißt $(G, \star, \epsilon)$ **Monoid**
c) gilt zusätzlich: $\forall g \in G \; \exists g' \in G : g \star g' = g' \star g = \epsilon$, so heißt $(G, \star, \epsilon, ')$ **Gruppe**

Behauptung:
ϵ in Teil b) und g' in Teil c) sind eindeutig.

Beweis:
Sei ein $\epsilon' \neq \epsilon \in G$ mit der Eigenschaft b), d.h. $\forall g \in G : \epsilon' \star g = g \star \epsilon' = g$, insbesondere gilt $(g = \epsilon) \; \epsilon' = \epsilon' \star \epsilon = \epsilon$ was ein Widerspruch zu $\epsilon' \neq \epsilon$ ist.$\square$
analog beweist man die Behauptung für g'.
Bezeichnungen: man schreibt $\cdot$ statt $\star$ und in $(G, \cdot)$ schreibt man $1 := \epsilon$ und $g^{-1} := g'$
bzw. in $(G, +)$ schreibt man $0 := \epsilon$ und $-g := g'$.
Das $+$ verwendet man bei abelschen (=kommutativen) Gruppen.
$(G, +)$ heißt abelsch $\Leftrightarrow \forall g_1, g_2 \in G : g_1 \cdot g_2 = g_2 \cdot g_1$

Lemma 1:
Ist $H = (H, \cdot, 1)$ ein Monoid, so ist $H^\star := \{h \in H | \exists h' \in H : h \cdot h' = h' \cdot h = 1\}$ eine Gruppe.

Beweis:
$H^\star \neq \emptyset$, weil $1 \in H^\star$. Denn
$h_1, h_2 \in H^\star \Rightarrow$
$h_1 \cdot h_1' = h_1' \cdot h_1 = 1$ und $h_2 \cdot h_2' = h_2' \cdot h_2 = 1 \Rightarrow$
$(h_1 \cdot h_2) \cdot (h_2' \cdot h_1') = 1 = (h_1' \cdot h_2') \cdot (h_2 \cdot h_1) \Rightarrow h_1 \cdot h_2 \in H^\star$.

Bemerkung:
a) In einer Gruppe $(G, \cdot)$ gilt $(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}$.
b) Sei M $\neq \emptyset$ eine Menge und $H = M^M =$ Abb (M, M) , dann ist $(H, \circ, id_M)$ ein Monoid, wobei $f \circ g$ durch $\forall x : (f \circ g)(x) := f(g(x))$ definiert ist und außerdem $\forall x : id_M(x) = x$ ist.
$H^\star = \{f \in H | f \text{ bijektiv}\} = Sym_M$ heißt auch symmetrische Gruppe auf M.
Die Elemente von Sym_M heißen Permutationen von M. Falls $M = \{1, \ldots, n\}$ gilt $Sym_M = S_n$.
b) Sei K ein Körper, dann ist $H = K^{n \times n} = \left\{ \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \middle| a_{ij} \in K \right\}$, so ist $(K^{n \times n}, \cdot, E_n)$ ein Monoid mit
$E_n = \begin{bmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{bmatrix}$ als Einselement.
Und $(GL_n(K), \cdot, E_n, ^{-1})$ ist eine Gruppe , wobei $GL_n(K) = GL(n, K) = H^\star = \{A \in K^{n \times n} | \det(A) \neq 0\}$.
c) $(\mathbb{Z}, +, 0)$ und allgemein $(R, +, 0)$ sind abelsche Gruppen, für beliebige Ringe R.
d) Sei V ein K-Vektorraum, dann ist $(V, +, \underline{0})$ ebenfalls eine abelsche Gruppe.
e) Sei wieder K ein Körper, dann ist $(SL_n(K), \cdot, E_n, ^{-1})$ eine Gruppe und zwar eine Untergruppe von $GL_n(K)$, dabei ist

$SL_n(K) = SL(n,K) = \{A \in K^{n\times n} | \det(A) = 1\}$.

Definition :
Ist $(G,\cdot)$ eine Gruppe, so ist $H \subseteq G$ **Untergruppe** in Zeichen $H \leq G$, wenn $(H, \cdot|_{H\times H}, 1)$ eine Gruppe ist.

Lemma 2:
vorrausgesetzt G ist eine Gruppe:
$H \leq G \Leftrightarrow$
(a) $H \neq \emptyset$ und
(b) $a,b \in H \Rightarrow a \cdot b^{-1} \in H$

Beweis:
eigentlich ist zu zeigen:
1) $H \neq \emptyset$
2) $a,b \in H \Rightarrow a \cdot b \in H$, d.h. $\cdot|_{H\times H} : H \times H \to$ H! und nicht nur $\to G$
3) $1 \in H$
4) $a \in H \Rightarrow a^{-1} \in H$
zu 3) Nach (a) $\exists a \in H$, da $H \neq \emptyset$ und nach (b) gilt $a \cdot a^{-1} = 1 \in H$ also gilt 3) .
zu 4) Sei $b \in H$ (mit $a = 1$) gilt nach b) , daß $b^{-1} = 1 \cdot b^{-1} \in H$.
zu 2) Seien $a,b \in H$. Nach 4) ist auch $b^{-1} \in H$.
Wende nun (b) an mit $b \Rightarrow b^{-1}$, so $a \cdot (b^{-1})^{-1} \in H$, da stets $b = (b^{-1})^{-1}$ gilt.$\square$

2. Vorlesung vom 20.10.2000

Definition:
Sei $M \subseteq G$(Gruppe) , dann ist

$$\langle M \rangle = \bigcap_{M\subseteq H\leq G} H \leq G$$

die von M **erzeugte Untergruppe** von G.
Es gilt :
a) $M \subseteq \langle M \rangle$
b) $M \subseteq H \leq G \Rightarrow \langle M \rangle \leq H$
c) $\langle \emptyset \rangle = \{1\}$

Lemma 4:
$\langle M \rangle = \{g_1 \cdot \ldots \cdot g_n | n \in \mathbb{N}_0, g_i \in M \cup M^{-1}\}$, wobei $M^{-1} := \{g^{-1} | g \in G\}$ ist.

Beispiel:
Sei $g \in G$ ist $\langle g \rangle = \langle \{g\} \rangle = \{g^n | n \in \mathbb{Z}\}$

Definition:
G heißt **zyklisch** , wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$ und $\sigma(g) := |\langle g \rangle|$ heißt **Ordnung** von g.

Beispiel:
$n \geq 2 : S_n = \langle (12), (12\ldots n) \rangle$ mit $a = (12), b = (12\ldots n)$ so ist $bab^{-1} = (23) \in H$, der Menge aller Transpositionen.
Jedes $g \in S_n$ läßt sich schreiben als $g = h_1 \cdot \ldots \cdot h_n$ mit $h_i \in \{(j \quad j+1) | 1 \leq j < n\} \subseteq H$.

1.2 Operationen von Gruppen auf Mengen

Sei $G = (G, \cdot, 1, ^{-1})$ eine Gruppe.

Definition:
G **operiert** auf M (von links) bzw. M ist G-Menge bzgl. einer
Abbildung $\star : G \times M \to M$, $(g,x) \mapsto g \star x$, wenn $\star$ die Eigenschaften
(a) $\forall x \in M$: $1 \star x = x$ und
(b) $\forall g_1, g_2 \in G, \forall x \in M$: $(g_1 \cdot g_2) \star x = g_1 \star (g_2 \star x)$ besitzt.

Beispiele:
1) Sei M eine Menge. G = $Sym(M)$ operiert auf M, wobei $g \star_1 x := g(x)$.

2) G sei $GL_n(K)$ und $X = K^{n\times 1}$, dann $g \star_2 x := g\Box x \in X$ mit $\Box$ ist das Matrix-Vektorprodukt im $K^{n\times n} \times K^{n\times 1}$.
3) Operiert G auf M, so auch auf $\mathfrak{P}(M) = 2^M = \{X | X \subseteq M\}$ mit $g \in G$: $g \star_3 X := \{g \star x | x \in X\} \subseteq \mathfrak{P}(M)$
z.B. S_4 operiert auf $\mathfrak{P}(\{1,\ldots,4\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\},$
$\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}$. Sei $g = (123) \Rightarrow g\star_3\emptyset = \emptyset,\ g\star_3\{1\} = \{2\},\ g\star_3\{2\} = \{3\},\ g\star_3\{1,2\} = \{2,3\},$
$g \star_3 \{2,3,4\} = \{1,3,4\}$
4) G operiert auch auf dem karthesischen Produkt $M^n = \underbrace{M \times \ldots \times M}_{n}$ durch $g \star_4 (x_1,\ldots,x_n) := (g \star x_1, \ldots, g \star x_n)$

5) Eine beliebige Gruppe $(G,\cdot)$ operiert durch Linksmultiplikation $g_1 \star_5 g_2 := g_1 \cdot g_2$ auf G. Auch jede Untergruppe $H \leq G$ operiert durch Linksmultiplikation auf G.
6) Auch $g_1 \star_6 g_2 := g_2 \cdot g_1^{-1}$ operiert auf G. (a) Ist trivialerweise erfüllt, da $1^{-1} = 1$. und (b) gilt auch denn $(g_1 \cdot g_2) \star_6 x = x \cdot (g_1 \cdot g_2)^{-1} = x \cdot (g_2^{-1} \cdot g_1^{-1}) = (x \cdot g_2^{-1}) \cdot g_1^{-1} = g_1 \star_6 (x \cdot g_2^{-1}) = g_1 \star_6 (g_2 \star_6 x)$.
7) als 3.Operation von G auf G definieren wir wie folgt $\star_7 : G \star_7 G \to G$, $(g,x) \mapsto g \star_7 x := g \cdot x \cdot g^{-1}$. (a) und (b) lassen sich analog zu oben zeigen. Diese Operation heißt **Konjugation**.

Lemma 1:
Operiert G (Gruppe)[links] auf $X \neq \emptyset$, so ist für jedes $g \in G \quad \sigma_g : X \to X\ ,\ \ x \mapsto g \cdot x$ eine Permutation, d.h. $\sigma_g \in Sym(X)$ und es gilt: $\sigma_{g_1 \cdot g_2} = \sigma_{g_1} \circ \sigma_{g_2}$.

Beweis:
$\forall x \in X$: $(\sigma_{g^{-1}} \circ \sigma_g)(x) = \sigma_{g^{-1}}(\sigma_g(x)) = \sigma_{g^{-1}}(g \cdot x) = g^{-1} \cdot (g \cdot x) \overset{(b)}{=} (g^{-1} \cdot g) \cdot x = 1 \cdot x \overset{(a)}{=} x$ folglich gilt $\sigma_{g^{-1}} \circ \sigma_g = id_X$.
genauso ist $\sigma_g \circ \sigma_{g^{-1}} = id_X$, d.h. σ_g ist bijektiv und es gilt $\forall x \in X : \sigma_{g_1 \cdot g_2}(x) = (g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot \sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x)$.□

3. Vorlesung vom 23.10.2000

Nachtrag zu Paragraph 1.1

Satz 1:
Ist $G = \langle g \rangle$ zyklisch und $|G| = n < \infty$. Dann gilt $G = \{1, g, g^2, \ldots, g^{n-1}\}$, $g^n = 1$ und $g^{-1} = g^{n-1}$.

Beweis :
Sei m = $\min\{j \in \mathbb{N} | \exists i \in \mathbb{N}_0 : 0 \leq i < j \text{ und } g^i = g^j\}$, dann $(*) g^i = g^m$ mit $0 \leq i < m$, wäre $i \neq 0$, so multipliziere $(*)$ mit $g^{-1} \Rightarrow g^{i-1} = g^{m-1}$ wegen $0 \leq i-1 < m-1$ ist dies ein Widerspruch zur Minimalität von m. Also $g^m = g^0 = 1$, $g \in H = \{1, g, \ldots, g^{m-1}\} \leq G$.Falls $|H| = n$ ist, so folgt $H = G$. Außerdem gilt $1 = g^n = g \cdot g^{n-1} = g^{n-1} \cdot g \Rightarrow g^{-1} = g^{n-1}$.

Folgerung :
Sei $M \subseteq G$, wobei G eine Gruppe ist und jedes $g \in M$ endlich Ordnung hat, also $\sigma(g) < \infty$, so ist $\langle M \rangle = \{g_1 \cdots g_n | n \in \mathbb{N}_0, g_i \in M\}$, denn $g_i^m = 1$ und $g_i^{-1} = \underbrace{g_i \cdots g_i}_{m-1} = g_i^{m-1}$, d.h. zu jedem Element $g \in M$ ist das Inverse eine positive Potenz von g selbst.
G operiere auf M mittels einer Abbildung $\star : G \times M \to M, (g,x) \mapsto g \star x$, d.h.
(a) $\forall x \in M : 1 \star x = x$ und
(b) $\forall g_1, g_2 \in G, \forall x \in M : (g_1 \cdot g_2) \star x = g_1 \star (g_2 \star x)$.
Dann ist die Abbildung $\sigma_g : M \to M, x \mapsto g \star x$ bijektiv,d.h. $\sigma_g \in Sym_M$.

Definition:
Sind $(G,\cdot), (H,\cdot)$ Gruppen, so heißt eine Abbildung $\varphi : G \to H$ ein **(Gruppen-)Homomorphismus**, wenn
$\forall g_1, g_2 \in G : \varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$ gilt. Ist zusätzlich φ bijektiv, so heißt φ ein **Isomorphismus**. $G \cong H$ " isomorph " $\Leftrightarrow \exists \varphi : G \to H$ mit φ ist ein Isomorphismus.

Satz 2 :
a) operiert G auf M, so ist die im Lemma 1 definierte Abbildung $G \Rightarrow Sym_M, g \mapsto \sigma_g$ ein Homomorphismus.
b) Ist umgekehrt $\varphi : G \to Sym_M$ ein Homomorphismus, G eine beliebige Gruppe und $M \neq \emptyset$ eine beliebige Menge, so wird durch $\star : G \times M \to M, (g,x) \mapsto \varphi(g)(x)$ eine Operation von G auf M definiert.

Vorbemerkung :
Ist $\varphi : G \to H$ ein Homomorphismus, so ist $\varphi(1) = 1$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$.
Denn sei $g \in G : \varphi(1) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) = 1 \Rightarrow \varphi(g)^{-1} = \varphi(g^{-1})$ und es folgt $\varphi(g) = \varphi(1 \cdot g) = \varphi(1) \cdot \varphi(g) = 1 \cdot \varphi(g) \overset{|\cdot\varphi(g)^{-1}}{\Leftrightarrow} 1 = \varphi(1)$.

Beweis :
a) siehe Lemma 1

b) Sei $g \star x := \varphi(g)(x)$, so $\forall x \in M : 1 \star x = \underbrace{\varphi(g)(x)}_{id_M nach Vorbe.} = x$ d.h. das Kriterium (a) mit dem man zeigt, dass $\star$ eine Operation ist, ist erfüllt.
$(g_1 \cdot g_2) \star x = \varphi(g_1 \cdot g_2)(x) = (\varphi(g_1) \circ \varphi(g_2))(x) = \varphi(g_1)(\varphi(g_2)(x)) = g_1 \star (g_2 \star x).\square$

Definition
G operiert **treu** auf M, bedeutet $g_1 \neq g_2 \Rightarrow \sigma_{g_1} \neq \sigma_{g_2}$, d.h. $\exists x \in M : g_1 \star x \neq g_2 \star x$
$\Leftrightarrow \sigma_g : G \to Sym_M$ gemäß Lemma 1 ist injektiv.

Beispiel :
Die triviale Operation von G auf M, $\forall x \in M : g \star x = x$ ($\sigma_g = id_M$) ist nicht treu für $|G| > 1$.

Satz von Cayley :
Jede Gruppe $(G, \cdot)$ operiert durch Linksmultiplikation treu auf sich selbst, d.h. $\forall g, x \in G : g \star x = g \cdot x$ oder anders formuliert: Jede Gruppe $(G, \cdot)$ ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.

Beweis :
Gilt $g_1 \cdot x = g_2 \cdot x$ für alle (oder auch nur ein) $x \in G$, dann $\Rightarrow_{|\cdot x^{-1}} g_1 = g_2$. Also $\sigma_g : G \to Sym_G, g \mapsto \sigma_g$ ist injektiv und $G \to \{\sigma_g | g \in G\}, g \mapsto \sigma_g$ ist ein Isomorphismus.

1.3 Bahnen

im folgenden Paragraphen sei G stets eine Gruppe, die auf einer nicht-leeren Menge M operiert.

Definition :
Ist $x \in M$, so ist $G \star x := \{g \star x | g \in G\}$ die **Bahn** von x unter G.

Beispiel :
Sei $G = \{\delta : \mathbb{R}^2 \to \mathbb{R}^2, x \mapsto \begin{bmatrix} cos\,\theta & -sin\,\theta \\ sin\,\theta & cos\,\theta \end{bmatrix} x \,|\theta \in \mathbb{R}\}$, dann ist die Bahn von x , $G \star x$ der Orbit um den Nullpunkt durch den Punkt x und speziell $G \star \underline{0} = \{\underline{0}\}$

Bahnalgorithmus :
$G = \langle\, g_1, \ldots, g_r \,\rangle$ operiere auf M. Gesucht ist die Menge $G \star x$.
Initialisiere die Mengen E,T,B mit $E = \{g_1, \ldots, g_r, g_1^{-1}, \ldots, g_r^{-1}\}, T = \{x\}$ und $B = \emptyset$. Wenn die Ordnung aller $g \in G$ endlich ist, reicht es E mit $\{g_1, \ldots, g_r\}$ zu initialisieren.
`WHILE` $T \neq \emptyset$ `DO`
- `WäHLE` $y \in T$ `UND WENDE AUF y ALLE` $g \in E$ `AN`
- `FALLS` $g \star y \notin T \cup B$ `, SO ERSETZT` T `DURCH` $T \cup \{g \star y\}$
- `ERSETZE` T `DURCH` $T - \{y\}$ `UND` B `DURCH` $B \cup \{y\}$

`ENDWHILE`
Ist $T = \emptyset$, dann ist $B = G \star x$.

Beispiel :
$G = \langle \underbrace{(1,4)(2,3)}_{g}, \underbrace{(1,3,5)(2,4,6)}_{h} \rangle, M = \{1, \ldots, 6\}$
$E = \{g, h\}$ suche Bahn von x = 1.

	0	$T = \{1\}$	$B = \emptyset$
	1	$T = \{3, 4\}$	$B = \{1\}$
	2	$T = \{3, 6\}$	$B = \{1, 4\}$
Schritte :	3	$T = \{6, 2, 5\}$	$B = \{1, 4, 3\}$
	4	$T = \{2, 5\}$	$B = \{1, 4, 3, 6\}$
	5	$T = \{5\}$	$B = \{1, 4, 3, 6, 2\}$
	6	$T = \emptyset$	$B = \{1, 4, 3, 6, 2, 5\}$

z.B. gilt $(h \circ h \circ g)(1) = 2, (g \circ h)(1) = 2$, aber $g \circ h \neq h^2 \circ g$, wegen $g \circ h = (12)(3546)$ und $h^2 \circ g = (12)(3645)$.

4. Vorlesung vom 25.10.2000

Beispiel:
$a) SL_2(\mathbb{R})$ operiert auf $\mathcal{H} := \{z \in \mathbb{C} | z = a + ib, b > 0\}$ mittels der Vorschrift:
$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z := \frac{az+b}{cz+d} \leftarrow_{\neq 0}$. Dies ist wohldefiniert, da $\mathrm{Im}(cz + d) = c\mathrm{Im}(z) \neq 0$ also $cz + d \neq 0$ ist. Außerdem ist stets Im

$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z\right) = \frac{Im(z)}{|cz+d|^2} > 0$ und $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot z = z$. Man kann durch eine leichte Rechnung zeigen, daß auch das 2.Kriterium einer Operation erfüllt ist, denn $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \cdot \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z\right) = \frac{a'\frac{az+b}{cz+d}+b'}{c'\frac{az+b}{cz+d}+d'} = \frac{(a'a+b'c)z+\cdots}{\cdots} = \left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) \cdot z$

b) Sei $G = SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \det A = ad - bc \ = 1, a, b, c, d \in \mathbb{Z} \right\} = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle =: \langle d, t \rangle$

Übung: Zeigen Sie: Wenn G auf $\mathcal{H}$ operiert , dann gilt: $d \cdot z = \frac{-1}{z}$ und $t \cdot z = z + 1$.

c) Ist M eine G-Menge (d.h. G operiert auf M). Kann man für eine beliebige Menge X die Menge X^M = Abb(M,X) zu einer G-Menge machen? Wie muß $\star : G \times X^M \to X^M$ aussehen?

Seien $g \in G$ und $f \in X^M$. Wir definieren $\star$ durch $\forall m \in M : g \star f(m) := f(g^{-1} \cdot m)$, beachte $g \star f : M \to X$. Wir überprüfen unsere beiden Kriterien für Operationen:

a) $\forall m \in M : 1 \star f(m) = f(1^{-1} \cdot m) = f(1 \cdot m) = f(m) \Rightarrow 1 \star f = f$. Ok!

b) $\forall m \in M : (g_1 \cdot g_2) \star f(m) = f((g_1 \cdot g_2)^{-1} \cdot m) = f((g_2^{-1} \cdot g_1^{-1}) \cdot m) = f(g_2^{-1} \cdot (g_1^{-1} \cdot m)) = g_2 \star f(g_1^{-1} \cdot m) = g_1 \star (g_2 \star f)(m)$

Erinnerung:

$\star : G \times M \to M$ sei eine Operation von G auf M, dann lautet die Bahn von $x \in M : G \star x = \{g \star x | g \in G\}$

Definition:

Ist $M = G \star x$, so heißt M **transitive** G-Menge oder man sagt G operiert **transitiv** auf M. Es gilt: M ist transitive G-Menge $\Leftrightarrow \forall x, y \in M \, \exists g \in G : g \star x = y$

Beispiel:

$GL_n(\mathbb{K})$ operiert transitiv auf $\mathbb{K}^{n \times 1} - \{\underline{0}\}$. Ist $v \neq \underline{0} \in \mathbb{K}^{n \times 1}$, so existiert $A \in GL_n(\mathbb{K})$ mit $v = A \cdot e_1$.

Satz über die Bahnzerlegung

Jede G-Menge ist die disjunkte Vereinigung von Bahnen: $M = \biguplus_{i \in I} B_i$ d.h. $i, j \in I : i \neq j \Rightarrow B_i \neq B_j$.

Beweis:

Jedes $x \in M$ liegt in einer Bahn, nämlich in $G \star x$, d.h. $M = \bigcup_{x \in M} G \star x$. Bleibt noch zu zeigen, daß $\bigcup$ disjunkt ist bzw. daß $G \star x \cap G \star y \neq \emptyset \Rightarrow G \star x = G \star y$. Wir nehmen also $G \star x \cap G \star y \neq \emptyset$ für $x \neq y \in M$ an. Dann $\exists z \in G \star x \cap G \star y \Rightarrow z = g_1 \star x = g_2 \star y$ $\Rightarrow x = (g_1^{-1} \cdot g_2) \star y \Rightarrow \forall g \in G : g \star x = (g \cdot g_1^{-1} \cdot g_2) \star y$, d.h. $G \star x \subseteq G \star y$ und aus Symmetriegründen auch $G \star y \subseteq G \star x$. Es gilt also $G \star x = G \star y$.□

Alternativ kann man dies auch beweisen, indem man eine Äquivalenzrelation $\sim$ auf M definiert durch $x \sim y :\Leftrightarrow \exists g \in G : y = g \star x$. Man zeige dann noch , daß $\sim$ eine Äquivalenzrelation ist. Die Äquivalenzklassen $[x]$ von $\sim$ sind dann die Bahnen wegen $[x]_\sim = \{y \in M | x \sim y\} = \{y \in M | \exists g \in G : y = g \star x\} = \{g \star x | g \in G\} = G \star x$.

1.4 Der Bahnensatz

im folgenden Paragraphen sei G stets eine Gruppe, die auf einer nicht-leeren Menge M operiert.

Definition:

Ist $x \in M$, so heißt $G_x = Stab_G(x) = \{g \in G | g \star x = x\}$ **Stabilisator** von x in G oder **Isotrophiegruppe** von x in G.

Lemma 1:

a) $G_x \leq G$

b) $G_{g \star x} = g \cdot G_x \cdot g^{-1} = \{g \cdot h \cdot g^{-1} | h \in G_x\}$

Beweis:

a) $1 = id \in G_x, g \in G_x \Rightarrow g^{-1} \in G_x$ und $g, h \in G_x \Rightarrow g \cdot h \in G_x$

b) $h \in G_{g \star x} \Leftrightarrow h \star (g \star x) = g \star x$

$\Leftrightarrow (g^{-1} \cdot h \cdot g) \star x = x$

$\Leftrightarrow g^{-1} \cdot h \cdot g = h' \in G_x$

$\Leftrightarrow h = g \cdot h' \cdot g^{-1} \in g \cdot G_x \cdot g^{-1}$.□

Definition:

Sind $H, H' \leq G$, so heißen H, H' in G **konjugiert** , wenn es $g \in G$ gibt mit $H' = g \cdot H \cdot g^{-1}$.

Also sind Stabilisatoren von Elementen in einer Bahn G-konjugierte Untergruppen.

Beispiel:

$G = D_8$ ist die Symmetriegruppe eines Quadrats im $\mathbb{R}^2$ mit $G = \{1, \delta, \delta^2, \delta^3, \sigma, \sigma', \tau, \tau'\} = \langle \delta, \sigma \rangle$. δ ist Drehung um $\frac{\pi}{2}$, σ, σ' sind Spiegelungen an den Achsen und τ, τ' sind Spiegelungen an den Diagonalen.

Dann operiert G auf $M := \{(x, y) | x, y \in \{0, 1, -1, \frac{1}{2}, -\frac{1}{2}\}\}$ und M ist auch eine G-Menge mit $|M| = 25$.

$4 = |G \star (1,0)| = |G \star (1,1)| = |G \star (\frac{1}{2}, \frac{1}{2})|$
$8 = |G \star (1, \frac{1}{2})|$
$1 = |G \star (0,0)|$
$G_{(1,0)} = Stab_G(1,0) = \{\sigma, 1\} = \langle\sigma\rangle = G_{(\frac{1}{2},0)}$
$G_{(1,1)} = \langle\tau\rangle$
$G_{(1,\frac{1}{2})} = \{1\}$
$G_{(0,0)} = G$

Definition:
Sei $U \leq G$, dann operiert U auf G durch Linksmultiplikation und die Bahnen $U \cdot g = \{u \cdot g | u \in U\}$ heißen **Rechtsnebenklassen** von U.
U operiert (von links) durch inverse Rechtsmultiplikation durch $u \star g = g \cdot u^{-1}$. Die Bahnen $\{g \cdot u^{-1} | u \in U\} =_{U \leq G} \{g \cdot u | u \in U\} = g \cdot U$ heißen **Linksnebenklassen** von U in G.

5. Vorlesung vom 27.10.2000

Definition:
Sei $U \leq G$ eine Gruppe und $gU = \{g \cdot u | u \in U\}$ die Linksnebenklassen von U in G, dann ist $G/U = \{g \cdot U | g \in G\}$ die Menge aller Linksnebenklassen von U in G.
Dann heißt $[G : U] := |G/U|$ **Index** von U in G.
Wenn M eine G-Menge ist, so $Stab_G(x) = G_x = \{g \in G | g \cdot x = x\} \leq G$.

Beispiel:
$$Stab_{SL_2(\mathbb{R})}(i) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R}) \middle| \frac{ai+b}{ci+d} = i \right\} = SO_2(\mathbb{R}) = \left\{ \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \middle| \theta \in \mathbb{R} \right\}$$

Bahnensatz :
G operiere auf $M \neq \emptyset$, dann gilt für ein $x \in M : |G \star x| = [G : Stab_G(x)] = [G : G_x]$.
in Worten: " Länge der Bahn = Index des Stabilisators ".
Außerdem ist die Abbildung $\mu : G \star x \to G/G_x$, $g \star x \mapsto gG_x$ eine Bijektion.

Beweis:
Ist für $g, h \in G, x \in M : g \cdot x = h \cdot x$
$\Leftrightarrow h^{-1} \cdot g \cdot x = x$
$\Leftrightarrow 1 = h^{-1} \cdot g$
$\Rightarrow h^{-1} \cdot g \in G_x$
Sei nun ein $s \in hG_x$, dann $\exists j \in G_x : s = h \cdot j$
$\Rightarrow \exists j' \in G_x : j = h^{-1} \cdot g \cdot j'$ und $s = h \cdot h^{-1} \cdot g \cdot j' = g \cdot j'$.
$\Rightarrow s \in gG_x$, also gilt $hG_x \subseteq gG_x$.
aus Symmetriegründen folgt auch die Inklusion $gG_x \subseteq hG_x$, d.h. $gG_x = hG_x$.
Damit ist μ wohldefiniert und auch injektiv ist. μ ist aber auch offensichtlich surjektiv .□

Satz 2: Satz von Lagrange
Ist $U \leq G$ und G eine endliche Gruppe. so ist $|G| = [G : U] \cdot |U|$.
Das bedeutet Ordnung und Index von U in G sind Teiler von $|G|$.

Beweis:
$g \cdot U$ ist Bahn $(= U \star g)$ von g unter der Operation $\star : U \times G \to G, (u, g) \mapsto g \cdot u^{-1}$.
Nach dem Satz der Bahnzerlegung von G ist : $G = \biguplus_{i \in I} g_i U$.
Dann ist $U_{g_i} = Stab_U(g_i) = \{u \in U | u \star g_i = g_i\} = \{u \in U | g_i \cdot u^{-1} = g_i\} = \{1\}$,
d.h. $|g_i \cdot U| = |U \star g_i| \overset{Bahnensatz}{=} [U : U_{g_1}] = [U : \{1\}] = |U|$, also $|G| = \sum_{i \in I} |g_i \cdot U| = |I| \cdot |U| = [G : U] \cdot |U|$.□

Folgerung:
a) Ist $g \in G$ eine endliche Gruppe, dann $\sigma(g) \mid |G|$
b) Ist $|G| = p$ Primzahl, so ist G zyklisch
c) Sei G endlich und M eine G-Menge, dann ist $\forall x \in M : |G \star x| \mid |G|$
d.h. die Länge der Bahn teilt die Gruppenordnung

Definition:
Seien $(X, \Diamond), (Y, \star)$ G-Mengen und G eine beliebige Gruppe.
Eine Abbildung $\mu : X \to Y$ heißt **G-Morphismus**, **G-verträglich** oder
G-äquivariant , wenn
$\forall x \in X \, \forall g \in G : \mu(g \Diamond x) = g \star \mu(x)$ ist.
Ist μ zusätzlich bijektiv, so heißt μ **G-Isomorphismus** (Notation : $X \cong_G Y$)

$:\Leftrightarrow \exists \mu : X \to Y$ und μ ist ein G-Isomorphismus.
Durch G-Isomorphismen wird eine Äquivalenzrelation auf der Menge aller G-Mengen definiert.

Satz 3: Klassifikation von transitiven Menge
a) Ist $U \leq G$, so wird G/U zu einer transitiven G-Menge durch die folgende Operation : $g \cdot \underbrace{(g'U)}_{\in G/U} := \underbrace{(g \cdot g')U}_{\in G/U}$.
b) Ist X transitive G-Menge und $x \in X$, so ist $X \cong_G G/G_x$
c) $U, V \leq G$, dann $G/U \cong_G G/V \Leftrightarrow \exists g \in G$ mit $V = gUg^{-1}$

Beweis:
zu a)
1)$\forall g_iU \in G/U : 1 \cdot (g_iU) = (1g_i)U = g_iU \surd$
2)$\forall g_1, g_2 \in G \forall hU \in G/U : (g_1 \cdot g_2)hU = (g_1 \cdot g_2 \cdot h)U = g_1 \cdot ((g_2 \cdot h)U) = g_1 \cdot (g_2 \cdot hU) \surd$
zu b)
Wir definieren μ wie in Satz 1. Es gilt $X = G \cdot x$, da X eine transitive Menge via Abbildung $\star$ ist. So $\mu(g \star x) = gG_x$ und für $g' \in G$ und $x \in X$ beliebig folgt, daß $\mu(g' \star (g \star x)) = \mu((g'g) \star x) = g'gG_x = g' \star \mu(g \star x)$.$\square$
zu c)
$\Rightarrow$: Sei $\mu : G/U \to G/V$ ein G-Isomorphismus , dann ist $\exists g \in G : \mu(1U) = gV$ und $u \in U : 1U = uU = u1U$.
zusammen $gV = \mu(u1U) = u \cdot \mu(1U) = ugV \Leftrightarrow V = g^{-1}ugV \Leftrightarrow g^{-1}ug \in V$, bzw. $u \in gVg^{-1}$. D.h. es gilt $U \subseteq gVg^{-1}$, insbesondere gilt also $U = gVg^{-1}$, da man die andere Inklusion ganz analog zeigen kann.
$\Leftarrow$: Sei $V = gUg^{-1}$. Definiere μ so : $G/U \to G/V$ $g'U \mapsto g'gV$. Man stellt fest μ ist wohldefiniert und eine bijektiver G-Morphismus.$\square$

6. Vorlesung vom 30.10.2000

Beispiel:
$G = S_3 = \{1, (12), (13), (23), (123), (132)\}$ operiert von links auf $X = \{1, 2, 3\}$ oder z.B. auch auf $M = X^2 = X \times X$.
So ist $|M| = 9$ und für ein $\sigma \in G$ und $i, j \in X$ ist dann $\sigma(i, j) = (\sigma(i), \sigma(j))$.
$G \cdot (1, 1) = \{(1, 1), (2, 2), (3, 3)\} \subseteq M$, $G_{(3,3)} = \langle (12) \rangle$, $G \cdot (1, 2) = M - \{(1, 1), (2, 2), (3, 3)\}$, $G_{(1,2)} = \{1\} \overset{Bahnensatz}{\Rightarrow}$
$|G \cdot (1, 2)| = [G : \{1\}] = |G| = 6$, d.h. $M = G \cdot (1, 1) \uplus G \cdot (1, 2)$, wobei $G \cdot (1, 1) \cong_G G/\langle (23) \rangle$ bzw. $G \cdot (1, 2) \cong_G G/\{1\}$ sind.
Allgemein gilt für eine Untergruppe $U \leq G = S_3$ nach Lagrange $|U| \mid 6 = |G|$, d.h. $|U| \in \{1, 2, 3, 6\}$.
$|U| = 1 \Rightarrow U = \{1\}$
$|U| = 6 \Rightarrow U = G$
da 2 und 3 Primzahlen sind, sind die 2 bzw. 3-elementigen Untergruppe zyklisch, d.h. $U = \langle u \rangle$ mit $u \in U - \{1\}$.
$|U| = 2 \Rightarrow U = \langle (12) \rangle$ bzw. $U = \langle (13) \rangle$ oder $U = \langle (23) \rangle$
$|U| = 3 \Rightarrow U = \langle (123) \rangle = \langle (132) \rangle$
Es gilt z.B. $g(12)g^{-1} = (23)$ für $g = (13) = g^{-1}$ oder auch $h(12)h^{-1} = (13)$ für $h = (23)$.
Die 2-elementigen Untergruppen sind also zueinander konjugierte Untergruppen und $G = S_3$ hat bis auf Isomorphie 4 - transitive G-Mengen und zwar G/G , $G/\langle (12) \rangle$, $G/\langle (123) \rangle$ und $G/\{1\}$ mit jeweils 1, 3, 2, 6 Elementen;

1.5 Konjugiertenklassen

Annahme ist, daß G operiert (von links) auf G durch Konjugation:
${}^g{}_h := g \star h = g \cdot h \cdot g^{-1}$ [in der Literatur findet man auch von rechts ${}_h{}^g := g^{-1} \cdot h \cdot g$].

Definition:
Die Bahnen dieser Operation heißen **Konjugiertenklassen**. $G \star h = {}^G{}_h = \{g \cdot h \cdot g^{-1} | g \in G\}$ ist die Konjugiertenklasse von h in G.
Der Stabilisator $C_G(h) := Stab_G(h) = \{g \in G | ghg^{-1} = h\} = \{g \in G | gh = hg\}$ heißt **Zentralisator** von h in G. D.h. der Zentralisator enthält nur Elemente die bzgl. g kommutativ sind.

Satz 1:
Jede Gruppe ist die disjunkte Vereinigung von Konjugiertenklassen. Ist G endlich und sind $C_1, \ldots, C_r$ Konjugiertenklassen von G, so gilt die Klassengleichung $|G| = \sum_{i=1}^{r} |C_i| = \sum_{i=1}^{r} [G : C_G(g_i)]$.

Beispiel:
Sei G eine Gruppe mit Ordnung $|G| = 6$ und seien $C_1, \ldots, C_r$ die Konjugiertenklassen von G.
Dann $\sum_{i=1}^{r} |C_i|$ mit $|C_i|$ ist Teiler von $|G| = 6$.
Das ergibt die folgenden Möglichkeiten für die Wahl der $|C_i|$:

$$|G| = 6 = \begin{cases} 1+1+1+1+1+1 \\ 1+1+1+3 \\ 1+1+2+2 \\ 1+2+3 \\ 2+2+2 \\ 3+3 \\ 6 \end{cases}$$

$1+1+1+1+2$ fällt als Möglichkeit weg, da $|Z(G)|\,|G| = 6$, aber $|Z(G)| = |\{C_i | C_i \text{ Konj.klasse mit } |C_i| = 1\}| = 4$.

Beispiel: $G = D_8$ die Diedergruppe
So ist $G = \{1, \delta, \delta^2, \delta^3, \sigma, \sigma', \tau, \tau'\}$

g	G_g	$C_g(g)$
1	$\{1\}$	G
σ	$\{\sigma, \sigma'\}$	$\{1, \sigma, \delta, \delta^2, \sigma\delta^2\}$
τ	$\{\tau, \tau'\}$	$\{1, \tau, \delta^2, \tau\delta^2\}$
δ	$\{\delta, \delta^3\}$	$\{1, \delta, \delta^2, \delta^3\}$
δ^2	$\{\delta^2\}$	G

$|G_g| \cdot |C_G(g)| = |G| = 8$
Bemerkung:
$\{g\}$ ist eine Konjugiertenklasse $\Leftrightarrow G = C_G(g) \Leftrightarrow \forall h \in G : gh = hg$

Definition:
$Z(G) = \{g \in G | \forall h \in G : gh = hg\}$ heißt **Zentrum** von G.

Bemerkung:
Z(G) ist eine Untergruppe von G, deshalb ist $|Z(G)| = |\{C_i | C_i \text{ ist Konjugiertenklasse mit } |C_i| = 1\}|$ Teiler der Gruppenordnung $|G|$.
Definition:
G heißt endliche **p-Gruppe** , wenn $|G| = p^m$ (p Primzahl).

Satz 2:
Ist G endliche p-Gruppe, so ist $Z(G) \neq \{1\}$.

Beweis:
$p^n = |G| = \sum_{i=0}^{n} [\, G : C_G(g_i)\,]$, wobei $C_1, \ldots, C_n$ Konjugiertenklassen mit $[\, G : C_G(g_i)\,] = p^{m_i}$ und $m_i \leq n$ sind.
So gilt $p^n = |G| = \sum_{i=0}^{n} [\, G : C_G(g_i)\,] = \underbrace{1 + \ldots + 1}_{|\{\, i \,|\, m_i = 0\}| = |Z(G)|} + p \underbrace{\sum_{m_i > 0} \frac{[\, G : C_G(g_i)\,]}{p}}_{\in \mathbb{N}_0}$

$\Rightarrow p$ teilt $|Z(G)|$ also $Z(G) \neq \{1\}$.

7. Vorlesung vom 30.10.2000

Beispiel 1:
Sei $G = GL_2(K) = \{A \in K^{2\times 2} | \det A \neq 0\}$ und $|K| = q < \infty$.
$g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, ${}^{G}_{g} = \{A \in GL_2(K) | A \text{ hat g als Jordansche Normalform}\}$ und $h = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$. Wir wollen die Anzahl der Matrizen bestimmen, die A als Jordansche Normalform haben, also $|{}^{G}_{g}|$. Dazu bestimmen wir den Zentralisator $C_G(g)$ von g in G: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}$
$\Leftrightarrow \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix}$
$\Leftrightarrow c = 0 \wedge a = d \neq 0$
Es folgt , daß der Zentralisator von g gleich $C_G(g) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| b \in K, a \in K - \{0\} \right\}$ ist und damit $|C_G(g)| = |K| \cdot (|K| - 1) = q^2 - q$ ist. Da außerdem $|GL_2(K)| = (q^2 - 1) \cdot (q^2 - q)$ ist, folgt $|{}^{G}_{g}| = \frac{|GL_2(K)|}{C_G(g)} = \frac{(q^2-1)\cdot(q^2-q)}{q^2-q} = q^2 - 1$.

Beispiel 2:
Sei $G = S_n$, $\tau \in S_n$, $\sigma = (i_1 \ldots i_m)$ mit $i_j \in \{1, \ldots, n\}$ und $i_j \neq i_{j'}$ für $j \neq j'$, soll bedeuten : $\sigma(i_j) = i_{j+1}$ für $j \in \{1, \ldots, m-1\}$, $\sigma(i_m) = i_1$ und $\sigma(i_k) = i_k$ für $k \notin \{i_1, \ldots, i_m\}$.
$\tau\sigma\tau^{-1} = (\tau(i_1) \ldots \tau(i_m))$ bzw. ${}^{S_n}_{\sigma} = \{(j_1 \ldots j_m) \in S_n | (j_1 \ldots j_m) \text{ ist ein m - Zyklus }\}$, beachte für Produkte von Zyklen gilt stets $\tau(\sigma_1\sigma_2)\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1}$.
speziell für n=4 ergibt sich die folgende Zerlegung von S_4 in die Konjugiertenklassen :

C	$\lvert C\rvert$
$\{1\}$	1
$^G_{(12)}$	6
$^G_{(123)}$	8
$^G_{(1234)}$	6
$^G_{(12)(34)}$	3
	$24 = 4! = \lvert G\rvert$

G operiert auch auf $\mathfrak{U}(G) = \{U \leq G | U$ Untergruppe $\}$ durch Konjugation $g \star U = {}^g{}_U = \{gug^{-1} | u \in U\} = gUg^{-1} \leq G$.

Definition:
Der Stabilisator von U unter dieser Operation heißt **Normalisator** von U in G, kurz $N_G(U) = \{g \in G | {}^g{}_U = U\} = \{g \in G | gUg^{-1} = U\}$. Man beachte , daß $|\{{}^g{}_U | g \in G\}| = [G : N_G(U)]$ und $U \leq N_G(U)$ ist. Offensichtlich gilt für den Zentralisator $\{g \in G | \forall u \in U : gu = ug\} = C_G(U) \leq N_G(U)$.

1.6 Abzählen von Bahnen

Beispiel:

Gegeben sei eine Halskette mit 6 Perlen und ≤ 3 Farben.
Frage: Wie viele verschiedene Halsketten gibt es ?
Problem : eine Halskette wird durch Rotation oder Spiegelung keine andere !
Modell : Wir haben ein regelmäßiges Sechseck $\{1, \ldots, 6\}$ und betrachten die Menge $X = \{f : \underbrace{\{1, \ldots, 6\}}_{M} \to \underbrace{\{r, s, t\}}_{F}\} =$

$Abb(M, F)$ mit $|X| = |F|^{|M|} = 3^6$.
Auf X operiert die Diedergruppe des regelmäßigen Sechsecks der Ordnung $12 = |G|$, $G = \{1, \delta, \ldots, \delta^5, \sigma, \sigma', \sigma'', \tau, \tau', \tau''\}$ mittels der Operation $\star$ definiert durch $\forall m \in M : g \star f(m) := f(g^{-1}(m))$.
gesucht : Anzahl der Bahnen von G auf X.

Satz von Cauchy, Frobenius
G operiere auf X ($|G|, |X| < \infty$) , dann ist die Anzahl der Bahnen von G auf X genau $b = \frac{1}{|G|} \sum_{g \in G} |Fix_X(g)|$, wobei $Fix_X(g) := \{x \in X | g \cdot x = x\}$ ist.

Beweis:
$P = \{(g, x) | g \star x = x\}$ so $|P|$
$= \sum_{g \in G} |\{x \in X | g \star x = x\}| = \sum_{g \in G} |Fix_X(g)|$
$= \sum_{x \in X} |\{g \in G | g \star x = x\}| = \sum_{x \in X} |G_x|$.

Nach dem Bahnensatz existiert die Zerlegung von X in die b Bahnen X_i, kurz $X = \bigcup_{i=1}^{b} X_i$. $\Rightarrow |P| = \sum_{g \in G} |Fix_X(g)| = \sum_{x \in X} |G_x| = \sum_{i=1}^{b} \sum_{x \in X_i} |G_x|$, wobei die $X_i = G \star x_i$ ist und somit $|X_i| = [G : G_{x_i}]$. Man beachte , daß $\forall x \in X_i \exists g_i \in G : x = g_i \star x_i \Rightarrow G_x = G_{g_i \star x_i} = g_i G_{x_i} g_i{}^{-1}$, weil $h \in G_{g \star x} \Leftrightarrow h \star (g \star x) = g \star x \Leftrightarrow (g^{-1} \star h \star g) \star x = x \Leftrightarrow g^{-1} \star h \star g \in G_x$ $\Leftrightarrow h \in g G_x g^{-1}$ und es gilt $|g G_{x_i} g^{-1}| = |G_{x_i}|$. $|P| = \sum_{i=1}^{b} \sum_{x \in X_i} |G_x| = \sum_{i=1}^{b} \sum_{j=1}^{|X_i|} |G_{x_i}| = \sum_{i=1}^{b} |X_i| |G_{x_i}| = \sum_{i=1}^{b} [G : G_{x_i}] |G_{x_i}| \overset{Lagrange}{=} \sum_{i=1}^{b} |G| = b \cdot |G| \Rightarrow \sum_{g \in G} |Fix_X(g)| = b \cdot |G|$.□
Nun können wir das Beispiel mit der Halskette lösen , indem wir für alle $g \in G$ $|Fix_X(g)|$ bestimmen :

g	$\lvert Fix_X(g)\rvert$	$H = \{h \in G \lvert Fix_X(h) = Fix_X(g)\}$	$\lvert H\rvert$
1	$\lvert X\rvert = \lvert F\rvert^{\lvert M\rvert} = 3^6$	$\{1\}$	1
δ	$\lvert F\rvert = 3^1$	$\{\delta, \delta^5\}$	2
δ^2	$\lvert F\rvert^2 = 3^2$	$\{\delta^2, \delta^4\}$	2
δ^3	$\lvert F\rvert^3 = 3^3$	$\{\delta^3\}$	1
σ	$\lvert F\rvert^4 = 3^4$	$\{\sigma , \sigma' , \sigma''\}$	3
τ	$\lvert F\rvert^3 = 3^3$	$\{\tau , \tau' , \tau''\}$	3

$\Rightarrow b = \frac{1}{12} \cdot (1 \cdot 3^6 + 2 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3 + 3 \cdot 3^4 + 3 \cdot 3^3) = \frac{1104}{12} = 92$

8. Vorlesung vom 6.11.2000

Lemma 1:
Sind $g, g' \in G$ konjugiert , d.h. $\exists h \in G : g' = hgh^{-1}$, so ist $|Fix_X(g)| = |Fix_X(g')|$.

Beweis:
$x \in Fix_X(g) \Leftrightarrow g \cdot x = x \Leftrightarrow h \cdot g \cdot x = h \cdot x \Leftrightarrow h \cdot g \cdot h^{-1} \cdot h \cdot x = h \cdot x \Leftrightarrow g' \cdot (h \cdot x) = h \cdot x \Leftrightarrow h \cdot x \in Fix_X(g')$

Bemerkung:
$\star : X \to X\ ,\ x \mapsto h \cdot x$ liefert eine Bijektion auf X.

1.7 Der verfeinerte Bahnalgorithmus

Frage :
Wie berechnet man die Ordnung $|G|$ einer beliebige Gruppe G ?
G operiere auf M , so ist nach dem Bahnensatz für ein $x \in M$: $|G \star x| = [G : G_x]$
$|G| = \underbrace{|G \star x|}_{Bahnalgorithmus} \cdot \underbrace{|G_x|}_{gesucht}$
Ziel: Modifikation des Bahnalgorithmus um ein Erzeugendensystem S von G_x zu finden. Da G_x auf $M - \{x\}$ operiert , könnte der modifizierter Bahnalgorithmus sukzessive angewandt werden und so $|G|$ in Faktoren zerlegen.

Beispiel :

Definition:
$U \leq G, G = \biguplus_{i \in I} g_i U$, dann heißt $T = \{g_i | i \in I\}$ eine **(Links-)Transversale** oder **Linksnebenklassenvertretersystem** von U in G.

Bemerkung:
Ist $U = G_x = Stab_G(x)$ und T eine Transversale von U in G. $g_i \in T \Rightarrow g_i U = \{g \in G | gx = g_i x\}$. Zu jedem $x_i \in G \star x \longleftrightarrow G/U = G/G_x$ existiert genau ein $g_i \in T$ mit $g_i x = x_i$.

Verfeinerter Bahnalgorithmus:
Sei $G = \langle h_1, \ldots, h_n \rangle$, G operiere auf M , $x \in M$, $G_x = Stab_G(x)$ und $E = \{h_1, \ldots, h_n, h_1^{-1}, \ldots, h_n^{-1}\}$, falls $\forall i \in \{1, \ldots, n\}$: $|\langle h_i \rangle| < \infty$ ist so genügt $E = \{h_1, \ldots, h_n\}$
verfeinerter Bahnalgorithmus
Initialisiere $T' = \{x\}, B = \emptyset, S = \emptyset, t(x) := 1$
(1) Auf das erste Element y von T' , wende alle $h \in E$ an.
(i) Ist $h \cdot y \notin T' \cup B$, so $T' := T' \cup \{hy\}$ und setze $t(h \cdot y) = h \cdot t(y) \in G$
(ii) sonst setzte $S := S \cup \{t(h \cdot y)^{-1} \cdot h \cdot t(y)\} \subseteq G$
(2) Anschließend setze $T' := T' - \{y\}$ und $B := B \cup \{y\}$
(3) Ist $T' \neq \emptyset$ so gehe zu (1)
Ist $|G \star x| < \infty$ so terminiert der Algorithmus mit $B = G \star x$, $T = \{t(y) | y \in B\}$ die Transversale von G_x in G und $G_x = \langle S \rangle$.

Bemerkung:
Es werden sukzessive die Element $x, h_1 x, \ldots, h_m x, h_1 h_1 x, \ldots, h_m h_1 x, h_1 h_2 x, \ldots h_m h_2 x, \ldots$ erzeugt , falls $\underbrace{h_{i_1} \cdots h_{i_r} x}_{=:y}$ und $y \notin T' \cup B$ so wird $t(y) := h_{i_1} \cdots h_{i_r}$ gesetzt , das bedeutet , daß $t(y)$ unter allen $g \in G$ mit $g \cdot x = y$ eines mit minimaler Länge ist.

Definition:
Ist $G = \langle E \rangle$ und $g \in G$, so sei $l_E(g) := \min\{k \in \mathbb{N}_0 | g = g_1 \ldots g_k, g_i \in E\}$, $l_E(1) := 0$ und für $g_i \in E : l_E(g_i) := 1$

Beweis:
zu $\langle S \rangle \subseteq G_x$:
Sei $y \in M$ so gilt : $t(hy)^{-1} \overbrace{h \underbrace{t(y)x}_{=y}}^{=hy} = x$, da $t(hy)x = hy$ und t bijektiv ist. Also gilt $t(hy)^{-1} h t(y) \in G_x$.
zu $G_x \subseteq \langle S \rangle$
Sei also $g \in G_x$ beliebig zu zeigen ist , daß dann auch $g \in \langle S \rangle$ gilt. Wir beweisen dies per Induktion über die Länge $l_E(g) =: k$:
Induktionsanfang ($k = 0$) : Dann ist $g = 1 \in \langle S \rangle$, da 1 in jeder Untergruppe von G enthalten ist.
Induktionsschluss ($k > 0$): So ist $g = g_k \cdots g_1$ mit $g_i \in E$. Es sei weiter $x_j := g_j \cdots g_1 \cdot x$, also $x_0 = x, x_1 = g_1 \cdot x, \ldots, x_k = g \cdot x = x = x_0$. Man sieht leicht , daß stets $l_E(t(x_j)) \leq j$ erfüllt ist und für $m+1 = \min\{j \in \mathbb{N} | l_E(t(x_j)) < j\}$ gilt $l(t(x_j)) = j$ für $j \in 0, 1, \ldots, m$
Im Fall (ii) des Algorithmus wird bei $x_{m+1} = g_{m+1} x_m$ min , $t(x_{m+1})^{-1} g_{m+1} t(x_m)$ zu S hinzugefügt .
$\Rightarrow g = \underbrace{g_k \cdots g_{m+2} \cdot t(x_{m+1})}_{l_E < k} \cdot \underbrace{t(x_{m+1})^{-1} \cdot g_{m+1} \cdot t(x_m)}_{\in S} \cdot \underbrace{t(x_n)^{-1} \cdot g_m \cdots g_1}_{=:a}$. Da der erste Teil von g nach Induktionsvoraussetzung aus $\langle S \rangle$ ist bleibt nur noch zu zeigen $a \in S$:

im Fall (i) des Algorithmus gilt $t(x_m) = g_m t(x_{m-1})$,d.h. $a = t(x_{m-1})^{-1} \cdot g_m^{-1} \cdot g_m \cdot g_{m-1} \cdots g_1 = t(x_{m-1})^{-1} \cdot g_{m-1} \cdots g_1$, was nach Induktionsvoraussetzung aus $\langle S \rangle$ ist , da $l_E(a) < k$ ist.
im Fall (ii) des Algorithmus ist $a = \underbrace{t(x_m)^{-1} \cdot g_m \cdot t(x_{m-1})}_{\in S} \cdot \underbrace{t(x_{m-1})^{-1} \cdot g_{m-1} \cdots g_1}_{\in \langle S \rangle nachInd.} \cdot \square$

1.8 Normalteiler

9. Vorlesung vom 8.11.2000

Frage: $U \leq G$ Gruppe, wann wird $G/U = \{gU | g \in G\}$ mit $(g_1U) \star (g_2U) = g_1g_2U$ eine Gruppe ?

Beispiel:
$G = S_3$, $U = \langle (12) \rangle = \{1, (12)\}$
Es ist $(13)U = \{(13), (123)\} = (123)U$ und $(23)U = \{(23), (132)\} = (132)U$,aber $(13)U \star (23)U = (132)U \neq 1U = (123)U \star (132)U$, obwohl die Operanden gleich sind , ist das durch $\star$ definierte Produkt verschieden , d.h. $\star$ ist nicht wohldefiniert.

Definition:
Sei $A, B \subseteq G$ Teilmengen einer Gruppe G so ist $A \cdot B := \{a \cdot b | a \in A, b \in b\} \subseteq G$ das **Komplexprodukt** von A und B.

Frage:
Wann wird G/U mit $\cdot|_{G/U \times G/U}$ eine Gruppe ?
Wegen $(13)U \cdot (23)U = \{(13), (123)\} \cdot \{(23), (132)\} = \{(132), (23), (12), 1\} \notin G/U$, gilt $\cdot|_{G/U \times G/U} \nrightarrow G/U$, sondern $\rightarrow \mathfrak{P}(G) = 2^G$.
Die Abbildung $\star$ ist wohldefiniert
$\Leftrightarrow \forall g_1, g_1', g_2, g_2' \in G : \ g_1U \star g_2U = g_1'U \star g_2'U$, falls $g_1U = g_1'U$ und $g_2U = g_2'U$
$\Leftrightarrow \forall g_1, g_1', g_2, g_2' \in G : \ g_1^{-1}g_1' =: u \in U$ und $g_2^{-1}g_2' =: u' \in U \Rightarrow (g_1g_2)^{-1}g_1'g_2' \in U$ bzw. $g_2^{-1} \underbrace{g_1^{-1}g_1'}_{u} g_2' \in U$

$\Leftrightarrow \forall u \in U \, \forall g \in G : gug^{-1} \in U$

Definition:
Eine Untergruppe $U \leq G$ von G heißt **Normalteiler** von G , wenn aus $u \in N$ und $g \in G$ stets $gug^{-1} \in N$ folgt (Konjugation führt nie aus N heraus).

Lemma 1:
Äquivalent sind die folgenden 4 Aussagen für eine Untergruppe N von G
a) N $\stackrel{\triangle}{\subseteq} G$ $(\Leftrightarrow u \in N \Rightarrow {}^G_u \subseteq N)$
b) N ist die Vereinigung von Konjugiertenklassen
c) $\forall g \in G : \ gN = Ng$
d) $G = N_G(N) = \{g \in G | gNg^{-1} \subseteq N\}$
$= \{g \in G | u \in N \Rightarrow gug^{-1} \in N\}$

Beweis:
a) $\Rightarrow$ *b)* $(u \in N \Rightarrow {}^G_u \subseteq N) \Rightarrow \bigcup_{u \in N} {}^G_u \subseteq N$
b) $\Rightarrow$ *c)* Seien $u \in U, g \in G$ so ist $gug^{-1} = u' \in N$ nach Vor. , d.h. $\underbrace{gu}_{\in gN} = u'g \in Ng$ also $gN \subseteq Ng$ und analog $Ng \subseteq gN$.
c) $\Rightarrow$ *d)* Es sei $\forall g \in G : \ gN = Ng$, also gilt für $u \in N \, \exists u' \in N : \ gu = u'g$ d.h. $gug^{-1} = u' \in N$ bzw. $g \in N_G(N)$.
d) $\Rightarrow$ *a)* Es sei $G = N_G(N) = \{g \in G | \forall u \in N : \ gug^{-1} \in N\}$ also gilt $gug^{-1} \in N \forall g \in G \forall u \in N$

Beispiel:
1) G sei abelsch und $U \leq G \Rightarrow U \trianglelefteq G$
2) G beliebig $U \leq Z(G) = \{z \in G | zg = gz \forall g \in G\} \Rightarrow U \trianglelefteq G$
3) Ist $U \leq G$ und $[G : U] = 2 \Rightarrow U \trianglelefteq G$
4) $\{1\}$ und G sind die trivialen Normalteiler von G

Beweis:
zu 1), 2) und 4) trivialerweise erfüllt
zu 3) Sei also $2 = [G : U] = |\{gU | g \in G\}| = |\{Ug | g \in G\}| \Rightarrow G/U = \{\underbrace{U}_{=1U}, G - U\}$, ebenso zerfallen die Rechtsnebenklassen von U in $U1$ und $G - U \Rightarrow U \trianglelefteq G_\square$
speziell gilt bei der alternierenden Gruppe $A_n = \{\sigma \in S_n | sgn \, \sigma = 1\} : \ A_n \trianglelefteq S_n$, wegen $[S_n : A_n] = 2$

10. Vorlesung vom 10.11.2000

Definition:
Seien $(G,\cdot),(H,\cdot)$ zwei Gruppen und $\varphi: G \to H$ ein Homomorphismus, so ist **Kern** $\varphi = \{g \in G | \varphi(g) = 1\}$.

Homomorphiesatz:
a) Ist $N \trianglelefteq G$, so wird $G/N = \{gN | g \in G\}$ Gruppe durch $(g_1N)\cdot(g_2N) := g_1g_2N$ und $\pi = \pi_N : G \to G/N, g \mapsto gN$ ist ein surjektiver Homomorphismus, man sagt auch kanonischer Epimorphismus
b) Ist umgekehrt $\varphi : G \to H$ ein Homomorphismus , so ist Kern $\varphi \trianglelefteq G$, Bild $\varphi \leq H$ und es existiert genau ein Homomorphismus $\Phi : G/\text{Kern}\ \varphi \to H$ mit $\varphi = \Phi \cdot \pi_{Kern\varphi}$, der injektiv ist.

Beweis:
zu a) $\star$ ist wohldefiniert, weil $N \trianglelefteq G$ (siehe Anfang §)ist. Außerdem ist $\star$ assoziativ , das Einselement ist $1N = N$ und von gN ist $g^{-1}N$ das Inverse.
$\pi = \pi_N$ ist Homomorphismus $\Leftrightarrow \underbrace{\pi(g_1g_2)}_{=g_1g_2N} = \underbrace{\pi(g_1)}_{g_1N}\cdot\underbrace{\pi(g_2)}_{g_2N}$, Kern $\pi = \{g \in G | gN = 1N\} = N$
zu b) $u_1, u_2 \in$ Kern $\varphi \Leftrightarrow \varphi(u_1) = \varphi(u_2) = 1 \Rightarrow \varphi(u_1^{-1}u_2) = \varphi(u_1)^{-1}\cdot\varphi(u_2) = 1$ also $u_1^{-1}u_2 \in$ Kern $\varphi \leq G$, denn $1 \in$ Kern φ
Sei weiter $g \in G$ beliebig so ist $\varphi(gu_1g^{-1}) = \varphi(g)\underbrace{\varphi(u_1)}_{1}\varphi(g^{-1}) = 1 \Rightarrow u_1 \in$ Kern φ d.h. $g \in G \Rightarrow gu_1g^{-1} \in$ Kern φ .
Es gilt $1 = \varphi(1) \in$ Bild $\varphi \neq \emptyset$ und $\varphi(g_1), \varphi(g_2) \in$ Bild $\varphi \Rightarrow \varphi(g_1^{-1}g_2) = \varphi(g_1)^{-1}\varphi(g_2) \in$ Bild $\varphi \leq H$.$\square$
Man definiere $N =$ Kern $\varphi, \Phi : G/N \to N$ durch $\Phi(gN) = \varphi(g)$, dann gilt $gN = g'N \Leftrightarrow g^{-1}g' \in N \Leftrightarrow \varphi(g^{-1}g') = 1 \Leftrightarrow \varphi(g)^{-1}\varphi(g') = 1 \Leftrightarrow \varphi(g) = \varphi(g')$, beachte Φ hängt nicht ab von der Wahl der Repräsentanten
" $\Rightarrow$ " bedeutet Φ ist wohldefiniert
" $\Leftarrow$ " bedeutet Φ ist injektiv
So ist $\varphi(g) = \Phi(\pi_N(g))$ bzw. $\varphi = \Phi \circ \pi_N$. Φ ist ein Homomorphismus , weil $gN, g'N \in G/N \Rightarrow \Phi(gN \cdot g'N) = \Phi(gg'N) = \varphi(gg') = \varphi(g)\varphi(g') = \Phi(gN)\Phi(g'N)$

Folgerung :
Jedes homomorphe Bild von G ist isomorph zu einer Faktorgruppe G/N mit $N \trianglelefteq G$.

Beispiel :
a) $G = S_3$ hat die folgenden Normalteiler :

N	G/N
$\{1\}$	$G/\{1\} \cong G$
A_3	$S_3/A_3 \cong S_2$
S_3	$S_3/S_3 \cong \{1\}$

b) Sei sgn : $S_n \to \{-1,1\}$ die Signumabbildung , so ist $sgn = \Phi \circ \pi_n$, wobei $\pi_n : S_n \to S_n/A_n$ der kanonische Epimorphismus und $\Phi : S_n/A_n \to \{-1,1\}$ ein Isomorphismus ist.

c) $G = S_4$

N	G/N
$\{1\}$	$G/\{1\} \cong G$
A_4	$G/V_4 \cong S_2$
S_4	$G/S_4 = \{1\} \cong \{1\}$

Satz 2 :
a) Ist $\varphi : G \to H$ ein Homomorphismus und $M \trianglelefteq H$, dann ist $\varphi^{-1}(M) = \{g \in G | \varphi \in M\} \trianglelefteq G$ und $\varphi^{-1}(\{1\}) =$ Kern φ
b) Ist $\varphi : G \to H$ Homo. und $N \trianglelefteq G$, so ist $\varphi(N) \trianglelefteq \varphi(G) =$ Bild (G)
c) Ist $U \leq G$ so ist $Core_G(U) := \bigcap_{g\in G} gUg^{-1} \trianglelefteq G$

Beweis :
a) $1 \in M, 1 \in \varphi^{-1}(M) \neq \emptyset$
$u_1, u_2 \in \varphi^{-1}(M) \Leftrightarrow \varphi(u_1), \varphi(u_2) \in M \Rightarrow \varphi(u_1)^{-1}\varphi(u_2) \in M \Rightarrow \varphi(u_1^{-1}u_2) \in M \Rightarrow u_1^{-1}u_2 \in \varphi^{-1}(M)$, es folgt daß $\varphi^{-1}(M) \leq G$
Sei $M \trianglelefteq H$ und $g \in G$: $\varphi(gu_1g^{-1}) = \varphi(g)\varphi(u_1)\varphi(g^{-1}) \overset{M\trianglelefteq H}{\Rightarrow} \varphi(u_1) \in M \Rightarrow u_1 \in \varphi^{-1}(M)$ also $gu_1g^{-1} \in \varphi^{-1}(M) \trianglelefteq G$
b) $N \trianglelefteq G$, $\varphi(g) \in \varphi(G), \varphi(u) \in \varphi(N) \Rightarrow \varphi(g)\varphi(u)\varphi(g)^{-1} = \varphi(\underbrace{gug^{-1}}_{\in N}) \in \varphi(N) \trianglelefteq \varphi(G)$
c) $y \in$ Kern $\varphi_u \Leftrightarrow \varphi_u(y) = id_{G/U} \Leftrightarrow \forall gU \in G/U, g \in G : \underbrace{\varphi_u(y)(gU)}_{ygU} = gU \Leftrightarrow g^{-1} \Leftrightarrow \forall g \in G : g^{-1}yg \in U \Leftrightarrow y \in gNg^{-1} \Leftrightarrow$
$y \in \bigcap_{g\in G} gUg^{-1}$

1.9 Gruppen mit Operatorenbereich

11. Vorlesung vom 13.11.2000

Definition :
Ω sei eine Menge, $(G,\cdot)$ eine Gruppe und $\star : \Omega \times G \to G$, $(\omega, g) \mapsto w \star g$ eine Abbildung mit
(1) $\forall g_1, g_2 \in G, \forall \omega \in \Omega : \ \omega \star (g_1 \cdot g_2) = (\omega \star g_1) \cdot (\omega \star g_2)$
Dann heißt $(G, \cdot, \Omega, \star)$ eine $\Omega-$**Operatorgruppe** bzw. Gruppe mit Operatorbereich Ω.

Bemerkung :
Es folgt aus (1) $\omega \star 1 = 1$ und $(\omega \star g)^{-1} = \omega \star g^{-1}$,denn $1 = \omega \star 1 = \omega \star (g \cdot g^{-1}) = (\omega \star g) \cdot (\omega \star g^{-1}) \Rightarrow (\omega \star g)^{-1} = \omega \star g^{-1}$

Beispiel :
a) Jede Gruppe $(G,\cdot)$ ist für Ω beliebig eine $\Omega-$Operatorgruppe mit $\star : \Omega \times G \to G$, $\forall \omega \in \Omega, g \in G : w \star g = g$
b) $(R, +, \cdot)$ sei Ring (z.B. Körper) und $M = (M, +, \cdot)$ ein R-Modul (z.B. Vektorraum) , dann ist M genauer $(M, +, R, \cdot)$ eine R-Operatorgruppe , da $\forall \omega \in R$ gilt : $w \cdot (v_1 + v_2) = \omega \cdot v_1 + \omega \cdot v_2$
c) Ist $(G,\cdot)$ eine Gruppe , so wird G zu einer G-Operatorgruppe $(G, \cdot, G, \star)$ durch $\star : G^2 \to G$, $(\gamma, g) \mapsto \gamma g \gamma^{-1}$, weil $\gamma \star 1 = \gamma \cdot \gamma^{-1} = 1$ und $\gamma \star (g_1 g_2) = \gamma g_1 g_2 \gamma^{-1} = \gamma g_1 \gamma^{-1} \gamma g_2 \gamma^{-1} = (\gamma \star g_1) \cdot (\gamma \star g_2)$ ist

Definition :
Ist $(G, \cdot, \Omega, \star)\, \Omega-$Operatorgruppe und $U \leq G$, dann heißt U Ω**-zulässig** oder Ω**-invariant** in Zeichen $U \leq_\Omega G$, wenn $\omega \in \Omega, u \in U \Rightarrow \omega \star u \in U$ gilt.
Ist auch $(H, \cdot, \Omega, \star)\, \Omega-$Operatorgruppe und ist $\varphi : (G,\cdot) \to (H,\cdot)$ ein Gruppenhomomorphismus bzw. Gruppenisomorphismus , so heißt φ ein Ω**-Homomorphismus** bzw.
Ω**-Isomorphismus** , wenn $\forall \omega \in \Omega, g \in G : \varphi(\omega \star g) = \omega \star \varphi(g)$. Man schreibt $G \cong_\Omega H$ gdw. $\exists\, \Omega-$Isomorphismus $\varphi : G \to H$

Beispiel :
a) Sei V ein R-Modul , so $U \leq_R V \Leftrightarrow$ U ist Untermodul von V (bzw. Teilraum von V falls V Vektorraum)
b) Sei V ein K-Vektorraum $\varphi \in \mathrm{End}(V)$ und $\Omega = \underbrace{K}_{Skalare} \cup \underbrace{\{\varphi\}}_{lin.Abb.}$ so ist $(V, +, \Omega, \star)$ eine $\Omega-$ Operatorgruppe mit
$\star : w \star v = \begin{cases} \omega \cdot v \ , \ \omega \in K \\ \varphi(v) \ , \ w = \varphi \end{cases}$
$U \leq_\Omega V \Leftrightarrow U$ ist $\varphi-$invarianter Teilraum im Sinne von LA
c) Sei $(G,\cdot)$ eine Gruppe betrachtet als G-Operatorgruppe mit $\gamma \star g = \gamma g \gamma^{-1}$, so gilt $U \leq_G G \Leftrightarrow U \trianglelefteq G$

Homomorphiesatz :
Sei G eine $\Omega-$Operatorgruppe .
a) Ist $N \leq_\Omega G$, so wird G/N zu einer $\Omega-$Operatorgruppe mit $\forall \omega \in \Omega, g \in G : \omega \star (gN) = (w \star g)N$ und $\pi : G \to G/N$, $g \mapsto gN$ ist $\Omega-$Homomorphismus mit Kern $\varphi = N$
b) Ist $\varphi : G \to H$ $\Omega-$Homomorphismus, so ist $N :=$ Kern $\varphi \leq_\Omega G$ und es existiert genau ein $\Omega-$Isomorphismus $\Phi : G/N \to$ Bild $\varphi \leq H$ mit $\forall g \in G : \Phi \circ \pi_N(g) = \varphi(g)$

Beweis :
a) $\star$ ist wohldefiniert : $g_1 N = g_2 N \Leftrightarrow g_1^{-1} g_2 \in N \overset{N \leq_\Omega G}{\Rightarrow} \omega \star (g_1^{-1} g_2) = (\omega \star g_1^{-1})(\omega \star g_2) = (\omega \star g_1)^{-1}(\omega \star g_2) \in N$
$\omega \star ((gN) \cdot (g'N)) = \omega \star (gg')N = ((\omega \star g)(\omega \star g'))N = (\omega \star gN) \cdot (\omega \star g'N)$
b) Sei $\varphi : G \to H$ ein $\Omega-$Homomorphismus und $g \in$ Kern $\varphi, \omega \in \Omega$, so $\varphi(\omega \star g) = \omega \star \varphi(g) = \omega \star 1 = 1$,
d.h. $\omega \star g \in$ Kern $\varphi \leq_\Omega G$. Ist nun Φ der $\Omega-$Isomorphismus, so $\Phi(\omega \star gN) = \Phi((\omega \star g)N) = \varphi(\omega \star g) = \omega \star \varphi(g) = \omega \star \Phi(gN)$.$\square$

Satz 1 :
Sei $\varphi : G \to H$ ein $\Omega-$Homomorphismus, so
a) Ist $V \leq_\Omega H \Rightarrow \varphi^{-1}(V) \leq_\Omega G$
b) $U \leq_\Omega G \varphi(U) \leq_\Omega H$

Beweis :
klar

1.10 Die Isomorphiesätze

1. Isomorphiesatz :
G sei eine $\Omega-$Operatorgruppe , $U \leq_\Omega G$ eine Untergruppe und N $\trianglelefteq_\Omega G$ ein Normalteiler in G, dann ist
$(N \trianglelefteq_\Omega) N \cdot U = \{n \cdot u | n \in N, u \in U\} \leq_\Omega G$,

$N \cap U \trianglelefteq_\Omega U$ und $U/N \cap U \cong_\Omega N \cdot U/N$.

Beweis :
zur Behauptung $U \cdot N \leq_\Omega G$:
Seien $xu, yv \in NU$, d.h. $x, y \in N$, $u, v \in U$, so gilt $(xu)^{-1}(yv) = u^{-1}x^{-1}yv = (\underbrace{u^{-1}xu}_{\in N})(\underbrace{u^{-1}yu}_{\in N})(\underbrace{u^{-1}v}_{\in U}) \in NU$.
Weiter gilt $\omega \in \Omega \Rightarrow \omega \star (xu) = (\underbrace{w \star x}_{\in N})(\underbrace{\omega \star u}_{\in U}) \in NU$, d.h. NU ist $\Omega-$invariant .$\square$
$\varphi : U \to NU/N$, $u \mapsto uN$ ist ein surjektiver $\Omega-$Homomorphismus , denn $xvN = vv^{-1}xvN = vN = \varphi(v)$ mit Kern $\varphi = U \cap N$, also ist nach dem Homomorphiesatz $\varphi(U) = NU/N \cong_\Omega U/\text{Kern } \varphi = U/N \cap U$.$\square$

12. Vorlesung vom 15.11.2000

Beispiel :
a) V sei K-Vektorraum ($\Omega = K$) und U_1, U_2 Teilräume (hier (V,+)=(G,$\cdot$)) , so $U_1 + U_2/U_1 \cong_K U_2/U_1 \cap U_2$ bzw. $dim(U_1 + U_2) - dim(U_1) = dim(U_2) - dim(U_1 \cap U_2)$
b) Sei $G = S_4, V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq G, S_3 = \{1, (123), (132), (12), (23), (13)\} \leq S_4$, so ist $V_4 \cap S_3 = \{1\}$ und $V_4 \cdot S_3/V_4 \cong S_3/\{1\} \cong S_3$, außerdem $|V_4 \cdot S_3| = [V_4 \cdot S_3 : V_4] \cdot |V_4| = 24$ also $V_4 \cdot S_3 = S_4$ und $S_4/V_4 \cong S_3$

Bezeichnungen :
$\mathfrak{U}(G) = \{U | U \leq_\Omega G\}$ ist die Menge der $\Omega-$invarianten Untergruppen in G und $\mathfrak{U}^\Omega_{\geq H}(G) = \{U \leq_\Omega G | H \leq U\}$ sind Untergruppen in G, die H enthalten.

2. Isomorphiesatz :
Sei $\varphi : G \to H$ ein surjektiver $\Omega-$Homomorphismus und $K = \text{Kern } \varphi$ (also $H \cong G/K$ nach dem Homomorphiesatz).
Die Abbildung $\beta : \mathfrak{U}^\Omega_{\geq K}(G) \to \mathfrak{U}^\Omega(H)$, $U \mapsto \varphi(U)$ ist eine Bijektion.
Dabei ist $\beta(U) = \varphi(U) \cong U/K$ und es gilt $(K \leq)U \trianglelefteq_\Omega G \Leftrightarrow \beta(U) \trianglelefteq_\Omega H$ und $G/U \cong H/\varphi(U)$

Beweis :
§1.9 Satz 1 besagt , daß $U \leq_\Omega G \Rightarrow \varphi(U) \leq_\Omega H$ und $U \trianglelefteq_\Omega G \Rightarrow \varphi(U) \trianglelefteq_\Omega \varphi(G) = H$
Ist also $K \leq U \leq_\Omega G$ so ist $\varphi|_U : U \to \varphi(U)$ ein surjektiver Homomorphismus mit Kern $\varphi|_U = U \cap K = K$. Demnach ist $\varphi(U) \cong_\Omega U/K$.
Die Abbildung β ist injektiv, denn : $K \leq_\Omega U_1, U_2 \leq_\Omega G$, wir nehmen an , daß $\varphi(U_1) \subseteq \varphi(U_2)$. Dann ist zu zeigen $U_1 \subseteq U_2$.
Sei dazu $u_1 \in U_1 \Rightarrow \varphi(u_1) \in \varphi(U_1) \subseteq \varphi(U_2) \Rightarrow \exists u_2 \in U_2 : \varphi(u_2) = \varphi(u_1)$ also ist $1 = \varphi(u_1)^{-1}\varphi(u_2) = \varphi(\underbrace{u_1^{-1}u_2}_{=:h}) \Rightarrow u_1^{-1}u_2 \in$ Kernφ und $u_1 = u_2h^{-1} = u_2u_2^{-1}u_1$, aber $u_2h^{-1} \in U_2$, weil $K \subseteq U_2$. Also $u_1 \in U_2$ d.h. $U_1 \subseteq U_2$. Weil U_1 und U_2 nicht von einander ausgezeichnet sind, gilt auch die Inklusion $U_2 \subseteq U_1$ und somit $U_1 = U_2$.
β ist auch surjektiv : Sei $V \leq_\Omega H$ setze $U := \varphi^{-1}(U) = \{u \in U | \varphi(u) \in U\} \leq_\Omega G$ Kern $\varphi = K \leq U$ (da $1 \in V$) , d.h. $U \in \mathfrak{U}^\Omega_{\geq K}(G)$ und $\beta(U) = \varphi(U) = V$.$\square$

Definition :
Eine Menge M mit einer Relation $\leq$ heißt eine **partiell geordnete Menge** oder **Poset** , wenn
i) $a \leq b$ und $b \leq a \Rightarrow a = b$
ii) $a \leq b$ und $b \leq c \Rightarrow a \leq c$
$(M, \leq)$ heißt **Verband** , wenn zusätzlich gilt
iii) $a, b \in M : \exists a \vee b \in M : (a, b \leq c \Leftrightarrow a \vee b \leq c)$
und $\exists a \wedge b \in M : (a, b \geq c \Leftrightarrow a \wedge b \geq c)$

Beispiel :
Sei P eine Menge, so ist $M = \mathfrak{P}(P) = 2^P = \{U | U \subseteq P\}$ die Potenzmenge von P ein Verband mittels $\subseteq$ und $a \vee b = a \cup b$ bzw. $a \wedge b = a \cap b$.

Definition :
Sind $(M, \leq)$, $(M', \leq)$ Verbände , so heißt eine Abbildung $\beta : M \to M'$ ein **Verbandsisomorphismus** ,wenn β bijektiv und zusätzlich $U \subseteq V$ in $(M, \leq) \Rightarrow \beta(U) \subseteq \beta(V)$ in $(M', \leq)$.

2. Isomorphiesatz (2.Version) :
Ist $K \trianglelefteq_\Omega G$ so ist $\beta : \mathfrak{U}^\Omega_{\geq K}(G) \to \mathfrak{U}^\Omega(H)$, $U \mapsto \varphi(U)$ eine Bijektion. Und $K \leq U \leq_\Omega G \Leftrightarrow U/K \trianglelefteq_\Omega G/K$, dann $G/U \cong_\Omega (G/K)/(U/K)$ und β ist ein Verbandsisomorphismus.

13. Vorlesung vom 17.11.2000

Sei $K \leq_\Omega G$ Gruppe so sind $\mathfrak{U}^\Omega_{\geq K}(G) = \{U \leq_\Omega G | K \leq U\}$ und $\mathfrak{U}^\Omega(G) = \mathfrak{U}^\Omega_{\geq \{1\}}(G)$ Verbände mittels $\subseteq$ wobei $U_1 \wedge U_2 =$

$U_1 \cap U_2 \in \mathfrak{U}^{\Omega}_{\geq K}(G)$ und $U_1 \vee U_2 = \langle\, U_1 \cup U_2 \,\rangle$.

Beispiel :
Sei $(\mathbb{Z}, +)$ eine teilweise (hier total) geordnete Menge. Wir wissen $U \leq G \Leftrightarrow U = m \cdot \mathbb{Z}$ mit $m \in \mathbb{N}_0$ und $m \cdot \mathbb{Z} \subseteq n \cdot \mathbb{Z}$ $\Leftrightarrow n|m \Leftrightarrow m \in n \cdot \mathbb{Z}$
z.B. gilt $(4\mathbb{Z}/12\mathbb{Z})/(12\mathbb{Z}/12\mathbb{Z}) \cong 4\mathbb{Z}/12\mathbb{Z} = \{4 + 12\mathbb{Z}, 8 + 12\mathbb{Z}, 0 + 12\mathbb{Z}\}$ oder $\mathbb{Z} = 4\mathbb{Z} + 3\mathbb{Z}$, $12\mathbb{Z} = 4\mathbb{Z} \cap 3\mathbb{Z}$ und $4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$

1.11 Automorphismen

Definition :
Sei $(G, \cdot)$ ein Gruppe , so ist die Abbildung $\alpha : G \to G$ ein **Automorphismus** $\Leftrightarrow \alpha$ ist ein Isomorphismus.
Aut(G) $= \{\alpha : G \to G | \alpha$ ist Isomorphismus $\}$

Bemerkung :
(Aut(G),$\circ$) ist die sogenannte Automorphismengruppe von G auf sich.

Satz 1 :
Ist $a \in G$, so ist $\kappa_a : G \to G$, $g \mapsto aga^{-1}$ ein Automorphismus und $\kappa : G \to$Aut(G) , $a \mapsto \kappa_a$ ist ein Homomorphismus mit Kern $\kappa =$Z(G) , wobei Z(G) $= \{z \in G | \forall g \in G : zg = gz\}$ das Zentrum von G ist.

Beweis :
zu κ_a ist ein Automorphismus :
$\kappa_a(g_1g_2) = ag_1g_2a^{-1} = ag_1a^{-1}ag_2a^{-1} = \kappa(g_1) \cdot \kappa(g_2)$, d.h. κ_a ist ein Homomorphismus und außerdem bijektiv , weil $\kappa_a \cdot \kappa_{a^{-1}} = \kappa_{a^{-1}} \cdot \kappa_a = id_G$
Die Abbildung κ ist ebenfalls ein Homomorphismus , denn seien $a, b, g \in G$ beliebig , so $\kappa_{ab}(g) = abg(ab)^{-1} = a\kappa_b(g)a^{-1} = (\kappa_a \circ \kappa_b)(g)$
Es gilt Kern $\kappa = \{a \in G | \kappa_a = id_G\} = \{a \in G | \forall g \in G : \kappa_a(g) = g\} = \{a \in G | \forall g \in G : ag = ga\} =$ Z(G).

Bemerkung und Definition :
Jede Gruppe $(G, \cdot)$ kann als $\Omega-$Operatorgruppe für jede Teilmenge $\Omega \subseteq$ Aut(G) betrachtet werden , wobei $\alpha \in \Omega\, \forall g \in G : \alpha \star g = \alpha(g)$.
$U \leq_{AutG} G$ heißt **charakteristische Untergruppe** von G in Zeichen U char G $\Leftrightarrow U \leq G$ und $u \in U, \alpha \in$Aut G $\Rightarrow \alpha(u) \in U$.
Es gilt $U \leq_{InnG} G \Leftrightarrow U \trianglelefteq G$, wobei Inn G die inneren Automorphismen von G sind, d.h. die Menge aller Konjugationen.

Beispiel :
a) 1 char G und G char G b) Z(G) char G , denn sei $z \in$ Z(G) , $\alpha \in$ Aut G , so ist $\forall g \in G : \alpha(z) \cdot g = \alpha(z)\alpha(\alpha^{-1}(g)) = \alpha(z \cdot \alpha^{-1}(g)) = \alpha(\alpha^{-1}(g) \cdot z) = g \cdot \alpha(z)$
c) Gibt es in G genau eine Untergruppe U mit $|U| = m$, dann ist $UcharG$ wegen $|U| = |\alpha(U)|$ und $\alpha(U) \leq G \Rightarrow U = \alpha(U)$
d) Ist G eine beliebige Gruppe und $m \,|\, |G|$. Sei dann $\mathfrak{U}_m(G) = \{U \leq G | m = |U|\}$, so ist $\bigcap_{U \in \mathfrak{U}_m}$ char G

Satz 2 :
a) U_1 , U_2 char G $\Rightarrow U_1 \cdot U_2$ char G und $U_1, U_2 \trianglelefteq G \Rightarrow U_1 \cdot U_2 \trianglelefteq G$
b) U char V char G $\Rightarrow$ U char G
beachte es gilt nicht allgemein $U \trianglelefteq V \trianglelefteq G \Rightarrow U \trianglelefteq G$

Beispiel :
Seien $G = S_4$ und $V = V_4$, so $\langle\, (12)(34) \,\rangle \trianglelefteq V_4 \trianglelefteq S_4$, aber nicht $U = \langle\, (12)(34) \,\rangle \trianglelefteq S_4$,weil $\exists g \in S_4 : g(12)(34)g^{-1} = (13)(24) \notin U$ nämlich für g = (23).

14. Vorlesung vom 20.11.2000

Beweis :
a) nach dem Homomorphiesatz gilt $U_1, U_2 \trianglelefteq_\Omega G \Rightarrow U_1 \cdot U_2 \leq_\Omega G$, wende diesen für $\Omega =$Aut G bzw. Inn G an
b) Sei $\alpha \in$ Aut G so ist $\alpha|_V \in$ Aut V , weil V char G
Sei weiter $g \in G$ beliebig und $\kappa_g : x \mapsto gxg^{-1}$ bzw. $\kappa_g \in$ Inn G, so ist $\varphi_g = \kappa_g|_V \in$ Aut V und es ist wegen U char V : $u \in U, g \in G \Rightarrow \underbrace{\varphi_g(u)}_{gug^{-1}} \in U$ also $UcharG$.$\square$

1.12 Zyklische Gruppen und ihre Automorphismen

G zyklisch Gruppe $\Leftrightarrow G = \langle g \rangle = \{g^i | i \in \mathbb{Z}\}$ für ein $g \in G$. Man sieht , daß $\forall i, j \in \mathbb{Z} : g^i g^j = g^{i+j}$ ist , was uns einen Epimorphismus $\pi : (\mathbb{Z}, +) \to G$, $i \mapsto g^i$ liefert mit $G \cong \mathbb{Z}/$ Kern π gemäß Homomorphiesatz.

Satz 1 :
Jede Untergruppe U von $(\mathbb{Z}, +)$ ist von der Form $m \cdot \mathbb{Z}$ mit $m \in \mathbb{N}_0$.
Und jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/m\mathbb{Z}$ mit $m \in N_0$ ($|\mathbb{Z}/m\mathbb{Z}| = m$).

Beweis :
Ist $U \leq \mathbb{Z}$, so setze $m := min\{j > 0 | j \in U\} \neq \emptyset$, falls $U \neq \{0\}$. Wenn $U = \{0\} = 0\mathbb{Z}$, sonst existiert $m \in \mathbb{N} : m\mathbb{Z} \subseteq U$. Sei $u \in U$, so $\exists q, r \in \mathbb{Z}$, $U \ni u = q \cdot m + r$ und $0 \leq r < m$ und es ist $m\, qm \in U$ sowie $r = u - qm \in U$. Also ist $r = 0$ aufgrund der Minimalität von m, d.h. $U = m\mathbb{Z}$.$\square$

Satz 2 :
a) Jede Faktorgruppe und jede Untergruppe einer zyklischen Gruppe ist zyklisch
b) Ist $G = \langle g \rangle$ mit $|G| = m$, so ist $\sigma(g^i) = \sigma = \langle g^i \rangle = \frac{m}{ggt(i,m)}$ insbesondere ist $\langle g^i \rangle = \langle g \rangle$, wenn ggt (m,i) = 1
c) $G = \langle g^i \rangle, |G| = m$ so hat G zu jedem Teiler d von m genau eine Untergruppe der Ordnung d
d) Jede Untergruppe einer endlich zyklischen Gruppe ist charakteristisch

Beweis :
a) Mit $G = \langle g \rangle$, $\pi : G \to G/N$ und $N \leq G$ ist $G/N = \pi(G) = \{\pi(g^i) | i \in \mathbb{Z}\} = \{\pi(g)^i | i \in \mathbb{Z}\} = \langle \pi(g) \rangle$, d.h. G/N ist zyklisch
Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Form $m\mathbb{Z} = \langle m \rangle$ mit $m \in \mathbb{N}_0$ und jede Untergruppe von $\mathbb{Z}/m\mathbb{Z}$ ist von der Form $\underbrace{U/m\mathbb{Z}}_{zykl.Faktorgr.}$ mit $m\mathbb{Z} \subseteq \underbrace{U}_{=n\mathbb{Z}} \leq \mathbb{Z}$, d.h. $n \mid m$ und U = $\langle n \rangle$.
b) Seien d=ggt(m,i) , m = dm' , u = di' , so daß ggt(m', i') = 1 , dann ist $g^{im'} = g^{i'dm'} = g^{mi'} = (g^m)^{i'} = 1^{i'} = 1$ und $\sigma(g^i) = l \mid m$. Andererseits ist $1(g^i)^l = g^{il}$ also $\sigma(g) = m \mid il = di'l$ also $m' \mid i'l$ wegen $m = dm' \Rightarrow m' \mid l$, weil ggt(m' , i') = 1 . Insgesamt heißt das $m' \mid l$ und $l \mid m' \Rightarrow l = m'$.$\square$
c) Es ist $G \cong \mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{N}$, d.h. |{ Untergruppen von G }| = |{ Untergruppen von $\mathbb{Z}/m\mathbb{Z}$}| = $|\{n\mathbb{Z}/m\mathbb{Z} \mid n|m\}|$ = |{ Untergruppen $n\mathbb{Z} \leq \mathbb{Z} \mid m\mathbb{Z} \leq n\mathbb{Z}$}|
d) folgt aus c) mit Beispiel c) aus §1.11

Satz 3 :
Aut $(\mathbb{Z}_n, +) \cong (\mathbb{Z}_n^\star, \cdot)$, wobei $n \in \mathbb{N}$, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}_n^\star = \{i + n\mathbb{Z} | ggt(i, n) = 1\}$ die multiplikative Gruppe der Restklassen modulo n ist und es gilt $(i + n\mathbb{Z}) \cdot (j + n\mathbb{Z}) = i \cdot j + n\mathbb{Z}$.

Beweis :
Sei $G = \langle g \rangle \cong \mathbb{Z}_n$, d.h. $|G| = n$ und sei $\alpha \in$ Aut G . Dann ist $\alpha(g) = g^j \in G$ und $\alpha(g^i) = \alpha(g)^i = g^{j \cdot i}$, d.h. α ist durch $j + n\mathbb{Z}$ eindeutig bestimmt wegen $g^{j+n \cdot z} = g^j \cdot (g^n)^z = g^j \cdot 1^z = g^j$
α ist surjektiv , also $G = \langle g \rangle = \langle g^j \rangle$, demnach ist $\sigma(g^j) = \sigma(g) = n \Rightarrow$ ggt(n,j) = 1
Wir haben damit die folgende Bijektion Aut$G \to \{j + n\mathbb{Z} | ggt(n, j) = 1\}$ $\alpha \mapsto j$ wenn $\forall g \in G : \alpha(g) = g^j$ war.
Umgekehrt sei $j + n\mathbb{Z} \in \mathbb{Z}_n^\star$ so definiere $\alpha_j : G \to G$, $g^i \mapsto g^{ij}$, dann ist $\alpha_j \in$ ein Homomorphismus G in G.

15. Vorlesung vom 22.11.2000

Also α_j ist ein Homomorphismus , da $\forall x, y \in G : \alpha_j(xy) = (xy)^j \overset{G \cong \mathbb{Z} \, abelsch}{=} x^j y^j = \alpha_j(x)\alpha_j(y)$. Weiter gilt $\alpha_j = \alpha_k \Leftrightarrow \alpha_j(g) = \alpha_k(g) \Leftrightarrow g^j = g^k \Leftrightarrow g^{j-k} = 1 \Leftrightarrow (j - k) + m\mathbb{Z} = 1 + m\mathbb{Z}$, es bleibt noch zu zeigen , daß α_j surjektiv ist : α_j surjektiv $\Leftrightarrow G = \alpha_j(G) = \langle g^j \rangle \Leftrightarrow$ ggt(m,j) = 1
Insgesamt bedeutet dies (Aut$G, \circ$) ist isomorph zur primen Restklassengruppe $((\mathbb{Z}/mZ)^\star, \cdot)$ modulo m .

Definition :
Die **eulersche Phi-Funktion** ist für ein $m \in \mathbb{N}$ wie folgt erklärt $\varphi(m) := |\mathbb{Z}_m^\star| = |\{j \in \{1, \ldots, m\} | ggt(j, m) = 1\}|$.

Beispiel :
Sei p eine Primzahl, so gilt $\varphi(p) = p - 1$ und $\varphi(p^n) = p^n - |\{kp | k = 1, \ldots, p^{n-1}\}| = p^n - p^{n-1} = p^{n-1}(p - 1)$

Satz von Euler :
Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ so ist ggt(a,m) = 1 $\Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$.

Beweis :
beachte $a \equiv b \bmod$ m $:\Leftrightarrow a + m\mathbb{Z} = b + m\mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$

Und für $a \in Z$ ist $a^{\varphi(m)} + m\mathbb{Z} = (\underbrace{a + m\mathbb{Z}}_{\in \mathbb{Z}_m^\star})^{\varphi(m)} = 1 \in \mathbb{Z}_m^\star$, da $\varphi(m)$ nach Definition die Gruppenordnung von $\mathbb{Z}_m^\star$ ist und deshalb $\forall z \in \mathbb{Z}_m^\star : z^{\varphi(m)} = 1$.$\square$

Kleiner Satz von Fermat :
Ist p Primzahl und $a \in \mathbb{Z} \Rightarrow a^p \equiv a \bmod p$.

Beweis :
1. Fall : $p \mid a \Rightarrow a = p \cdot q$ und so $a^p - a = p(p^{p-1}q^p - q) \in p\mathbb{Z} \Rightarrow a^p \equiv a \bmod m$
2. Fall : $p \not| a$ dann $a + p\mathbb{Z} \in \mathbb{Z}_p^\star \overset{Euler}{\Rightarrow} a^{\varphi(p)} = a^{p-1} \equiv 1 \bmod p \overset{|\cdot a + m\mathbb{Z}}{\Rightarrow}$ Beh.
In §1.13 werden wir zeigen $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, falls $\text{ggt}(n, m) = 1$, z.B. $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400$

Beispiel :
Frage: Was sind die letzten 3 Ziffern von x $= 7^{432401}$?
Gesucht ist $n \in \{0, \ldots, 999\}$ mit $x + 1000\mathbb{Z} \equiv n + 1000\mathbb{Z}$, da ggt(7,1000)=1 $\overset{Euler}{\Rightarrow} 7^{\varphi(1000)} \equiv 1 \bmod 1000$, d.h. $7^{432400} \equiv (7^{400})^{1081} \equiv 1 \bmod 1000$ Also lautet die Antwort 007 .

1.13 Direkte Produkte und der chinesischer Restesatz

Definition :
Sind $G_1, \ldots, G_r$ Gruppen, so wird das karthesische Produkt $G_1 \times \cdots \times G_r = \{(g_1, \ldots, g_r) | g_i \in G_i\}$ zu einer Gruppe mit $(g_1, \ldots, g_r) \star (g_1', \ldots, g_r') = (g_1 \star_1 g_1', \ldots, g_r \star_r g_r')$, wobei $\star_i$ das Produkt in der Gruppe G_i bezeichnet. Man sieht sofort das Einselement in G ist $(1, \ldots, 1)$ und es ist $(g_1, \ldots, g_r)^{-1} = (g_1^{-1}, \ldots, g_r^{-1})$. $D = G_1 \overset{*}{\times} \cdots \overset{*}{\times} G_r$ heißt **direktes Produkt** . Ist weiter G eine Gruppe und sind $H_1, \ldots H_r$ Untergruppen von G mit mit einer Abbildung $\Phi : H_1 \times \cdots \times H_r \to G$, $(h_1, \ldots, h_r) \mapsto h_1 \cdots h_r = \Pi_{i=1}^r h_i$, so heißt Φ **inneres direktes Produkt** von $H_1, \ldots, H_r$ in Zeichen $H_1 \dot{\times} \cdots \dot{\times} H_r$, wenn Φ ein Isomorphismus ist.

Satz 1 :
Sind $H_i \leq G$, $1 \leq i \leq r$, so ist $G = H_1 \dot{\times} \cdots \dot{\times} H_r \Leftrightarrow$
i) $G = H_1 \cdots H_r$ und
ii) $H_i \trianglelefteq G$ für $1 \leq i \leq r$ und
iii) $H_i \cap H_1 \cdots H_{i-1} \cdot H_{i+1} \cdots H_r = \{1\}$

Beweis :
zu $\Rightarrow$:
zu i) Es gilt $G = H_1 \cdots H_r$, da Φ nach Definition surjektiv ist
zu iii) $H_i = \{\Phi(1, \ldots, h_i, \ldots, 1) | h_i \in H_i\}$ und $H_1 \cdots H_{i-1} H_{i+1} \cdots H_r = \{\Phi(h_1, \ldots, \underbrace{1}_{i} \ldots h_r) | h_j \in H_j\}$ Φ ist nach Annahme injektiv also gilt iii)
zu ii) $h \in H_i, g \in G \Rightarrow ghg^{-1} = \Phi(h_1, \ldots, h_r)\Phi(1, \ldots, h, \ldots, 1)\Phi(h_1^{-1}, \ldots, h_r^{-1}) = \Phi(h_1 h_1^{-1}, \ldots, h_i h h_i^{-1}, \ldots, h_r h_r^{-1}) = h_i h h_i^{-1} \in H_i$, d.h. ii) ist erfüllt
zu $\Leftarrow$:
Es mögen i),ii),iii) gelten. Zunächst zeigen wir $*) h_i h_j = h_j h_i$ für $i \neq j, h_i \in H_i, h_j \in H_j$ $1 \overset{!}{=} \underbrace{h_i^{-1}}_{\in H_i} \underbrace{h_j^{-1} h_i h_j}_{\in H_i \trianglelefteq G} = \underbrace{h_i^{-1} h_j^{-1} h_i}_{\in H_j \trianglelefteq G} \underbrace{h_j}_{\in H_j} \in$ $H_i \cap H_j = \{1\}$, also $h_i h_j = h_j h_i$
Wegen i) ist Φ surjektiv und es ist $\Phi((h_1, \ldots, h_r) \cdot (h_1', \ldots, h_r')) = \Phi(h_1 h_1', \ldots, h_r h_r') = h_1 h_1' \cdots h_r h_r' \overset{*)}{=} h_1 \cdots h_r h_1' \cdots h_r'$ $= \Phi(h_1, \ldots, h_r) \cdot \Phi(h_1', \ldots, h_r') \Rightarrow \Phi$ ist ein Homomorphismus . Der Kern $\Phi = \{(h_1, \ldots, h_r) | \underbrace{h_1 \cdots h_r = 1}_{\Rightarrow h_1^{-1} = h_2 \cdots h_r \in H_1 \cap H_2 \cdots H_r}\}$ nach iii) folgt $h_1^{-1} = 1$ und iteriert man diese Argumentation so erhält man $h_1 = h_2 = \ldots = h_r = 1$, d.h. Kern $\Phi = \{(1, \ldots, 1)\} = \{1\}$, d.h. Φ ist injektiv.$\square$

16. Vorlesung vom 24.11.2000

Seien $U_1, \ldots, U_r \leq G$ mit $U_1 \times \ldots \times U_r = G \Leftrightarrow \Phi : U_1 \times \ldots \times U_r \to G$, $(u_1, \ldots, u_r) \mapsto u_1 \cdots u_r$, d.h. jedes $g \in G$ ist eindeutig darstellbar als $g = u_1 \cdots u_r$ mit $u_i \in U_i$ und $(u_1, \ldots, u_r)(u_1', \ldots, u_r') = u_1 u_1' \cdots u_r u_r'$

Satz 1 :
$G = U_1 \times \ldots \times U_r \Leftrightarrow$

i) $G = U_1 \cdots U_r$ und
ii) $U_i \trianglelefteq G$ für $1 \leq i \leq r$ und
iii) $U_i \cap U_1 \cdots U_{i-1} \cdot U_{i+1} \cdots U_r = \{1\}$

Satz 2 :
a) Ist $\text{ggt}(m,n) = 1$, so ist $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$
b) Sind $m_1, \ldots, m_r$ paarweise teilerfremd , so ist $\mathbb{Z}_{m_1 \cdots m_r} \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$
$\Psi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$, $z \mapsto (z + m_1\mathbb{Z}, \ldots, z + m_r\mathbb{Z})$ ist Epimorphismus mit Kern $\Psi = m_1 \cdots m_r\mathbb{Z}$

Beweis :
a) Sei also $G = \mathbb{Z}_{mn}$ hat genau die Untergruppen $C_m, C_n \trianglelefteq G$ mit $|C_m| = m$ und $|C_n| = n$.
Nach Lagrange ist $\{1\} = C_m \cap C_n$ und $|C_m C_n| = \frac{m \cdot n}{1} = |G|$, d.h. $G = C_m C_n$ ist nach Satz 1 $G = C_m \times C_n$
b) Induktion $\Psi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ ist stets eine Homomorphismus mit Kern $\Psi = \{z | z \in m_1\mathbb{Z} \cap \ldots \cap m_r\mathbb{Z}\} = m_1 \cdots m_r\mathbb{Z}$, weil die m_i relativ prim sind.
Bild $\Psi \cong \mathbb{Z}/m_1 \cdots m_r\mathbb{Z} \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ hat Ordnung $|\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}|$, also ist Ψ surjektiv.

Folgerung (Chinesischer Restsatz) :
Sind $m_1, \ldots m_r \in \mathbb{N}$ relativ prim und $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig so existiert ein $z \in \mathbb{Z} : z \equiv a_i \mod m_i$ für $i \in \{1, \ldots, r\}$.
Ist z_0 eine Lösung der simultanen Kongruenzen so ist die Menge aller Lösungen $z_0 + m_1 \cdots m_r\mathbb{Z}$.

Beweis :
Ψ von Satz 2 ist surjektiv , also $\exists z \in \mathbb{Z}$ mit $\Psi(z) = (a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$
$\Psi(z) = \Psi(z') \Rightarrow z - z' \in \text{Kern } \Psi = m_1 \cdots m_r\mathbb{Z}$

Satz 3 :
Ist $\text{ggt}(m,n) = 1$, so ist $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, wobei φ die Eulersche $\varphi-$Funktion ist.

Beweis :
zu $\Rightarrow$:
$\varphi(n) = |\{i \in \{1, \ldots, n\} | ggt(i,n) = 1\}| = |\{g \in C_n | \langle g \rangle = C_n\}|$ =Anzahl der erzeugenden Elemente einer zyklischen Gruppe der Ordnung n, $|C_n| = n$
$\langle (g,h) \rangle = C_m \times C_n \Leftrightarrow C_m \times C_n = \{(g^i, h^i) | i \in \mathbb{Z}\} \Rightarrow \langle g \rangle = C_m$ und $\langle h \rangle = C_n$
zu $\Leftarrow$:
Sei $\langle g \rangle = C_m, \langle h \rangle = C_n$ und $\sigma(\langle g,h \rangle) = l$
zu zeigen $l = m \cdot n$: $(1,1) = (g,h)^0 = (g^l, h^l)$ also $m \mid l$, $n \mid l \Rightarrow m \cdot n \mid l$,da ggt(m,n) = 1 und $l \mid m \cdot n = |C_m \times C_n|$ nach Lagrange.

1.14 Die Sylowsätze

Lagrange : Für $|G| = n$ existiert $U \leq G, |U| = m \Rightarrow m | n$.

Frage :
Gilt die Umkehrung auch ?

Antwort :
Nein, nicht im Allgemeinen.

Beispiel :
$G = A_4$, $|A_4| = 12$ hat keine Untergruppe der Ordnung 6.

17. Vorlesung vom 27.11.2000

1. Satz von Sylow 1872 :
Ist $|G| = p^a r$ mit p Primzahl und $r \in \mathbb{N}$, so hat G eine Untergruppe der Ordnung p^a.

Lemma 1 :
G endl. Gruppe mit $|G| = n$, $1 \leq r \leq n$
$\mathbb{M} = \mathbb{M}_r(G) = \{M \subseteq G \mid r = |M|\}$
G operiert auf $\mathbb{M}$ durch Linksmultiplikation $g \cdot M = \{g \cdot x | x \in M\}$. Nach dem Satz über die Bahnzerlegung ist $\mathbb{M} = \bigcup_{i=1}^{n} G \cdot M_i$ disjunkt und $|G \cdot M_i| = \frac{n \cdot b_i}{m}$ wobei $b_i \mid m$. Außerdem $b_i = 1 \Leftrightarrow G \cdot M_i = G/U$

Beweis :
$G \cdot M_i = \{g_1 M_i, \ldots, g_m M_i\}$, $G = \{g_1, \ldots, g_m\}$
o.B.d.A. $1 \in M_i$,sonst wenn $g \in M_i$ ersetze M_i durch $g^{-1}M_i$
Setze $U_i = Stab_G M_i, u \in U_i$, so ist $uM_i = M_i$ und $u \in M_i$, also $U_i \subseteq M_i$.
M_i ist die Vereinigung von b_i Rechtsnebenklassen von U_i . $m = |M_i| = |U_i| \cdot b_i \Rightarrow b_i \,|\, m$ $|G \cdot M_i| = [G : U_i] = \frac{n}{\frac{m}{b_i}}$

Lemma 2 :
$|G| = n \geq m \geq 1$, $\mathbb{M} = \mathbb{M}(G) = \{M \subseteq G \,|\, |M| = m\}$, $|M| = \binom{n}{m}$
$\mathbb{M} = \biguplus_{i=1} G \star M_i$, $|G \star M_i| = \frac{n \cdot b_i}{m}$ mit $b_i | m$. Es ist $b_i = 1 \Leftrightarrow G \star M_i = G/U_i$ für eine Untergruppe $U_i \leq G$ und $|U| = m$.

1. Sylowsatz :
Ist $|G| = p^a r$, $r \in \mathbb{N}$, so existieren Untergruppen der Ordnung p^a , deren Anzahl $n_{p^a}(G) = \{U \leq G | p^a = |U|\} \equiv 1 \bmod p$ ist.

Beweis :
Wende Lemma 1 an auf $n = p^a r$ und $m = p^a$, so $\mathbb{M} = \mathbb{M}_m(G)$ mit $|\mathbb{M}| = \binom{p^a r}{p^a} = \sum_{i=1}^{r} |G \star M_i| = \frac{n}{m} \sum_{i=1}^{r} b_i$. Entweder ist $b_i = 1$, dann enthält $G \star M_i$ genau eine Untergruppe, oder $b_i > 1$ so teilt b_i aber $m = p^a$, d.h. $b_i = p^j$. Was wiederum heißt, daß $p | b_i$ und $\binom{p^a r}{p^a} \equiv \frac{n}{m} n_{p^a}(G) \bmod pr \equiv r n_{p^a}(G) \bmod$ pr . Dies gilt für jede Gruppe G mit $|G| = p^a r$, insbesondere auch für $G = C_{p^a r} \cong (\mathbb{Z}_{p^a r}, \cdot)$. Aus §1.12 wissen wir $n_{p^a}(C_{p^a r}) = 1$. Eingesetzt ergibt dies $\binom{p^a r}{p^a} \equiv r \cdot 1 \bmod pr \Leftrightarrow r \equiv r n_{p^a}(G) \bmod$ pr $\Leftrightarrow 1 \equiv n_{p^a r}(G) \bmod$ p.

Definition :
$Syl_p(G) = \{U \leq G | p^a\}$ ($\neq \emptyset$ nach Satz 1) , falls $|G| = p^a m$ mit $p \nmid m$.
$P \in Syl_p(G) \Leftrightarrow$ P ist **p-Sylowgruppe** von G.

2. Sylowsatz :
Sei $U \leq G$ mit $|U| = p^b$, p Primzahl und $S \in Syl_p(G)$. Dann existiert $g \in G$ mit $U \leq gSg^{-1}$ und insbesondere sind je zwei p-Sylowgruppen von G in G konjugiert.

Beweis :
(G und) U operieren auf G/S , $|G| = p^a m$ und $p \nmid m$. Jede U-Bahn hat als Länge eine p-Potenz. $|G/S| = \frac{p^a m}{p^a} = m = \sum_{i=1}^{r} |U \cdot (x_i S)|$ kein Vielfaches von p , da $p \nmid m$. $\exists i$ mit $|U x_i S| = 1$ so ist $\forall u \in U : u \cdot x_i S = x_i S \Leftrightarrow x_i^{-1} u x_i \in S \Leftrightarrow u \in x_i S x_i^{-1} \Rightarrow U \leq x_i S x_i^{-1}$

3. Sylowsatz :
Ist $|G| = p^a m$ mit $p \not| m$, so ist $n_{p^a}(G) = |Syl_p(G)|$ Teiler von m und kongruent 1 modulo p. Also kurz $n_{p^a}(G) | m$, $n_{p^a}(G) \equiv 1$ mod p.

Beweis :
$|Syl_p(G)| = |\{gSg^{-1} | g \in G\}| = [G : N_G(S)]$ mit $S \in Syl_p(G)$. Da $N_G(S) = \{g \in G | gSg^{-1} = S\} \geq S$ folgt , daß $|Syl_p(G)| = \frac{[G:S]}{[N_G(S):S]} = \frac{m}{[N_G(S):S]}$ und demnach Teiler von m ist.

Korollar :
Ist $P \in Syl_p(G)$, so sind die folgenden Aussagen äquivalent:
a) $Syl_p(G) = \{P\}$
b) $P \trianglelefteq G$
c) P char G

Beweis :
a) $\Rightarrow$ b) : $\forall g \in G : |gPg^{-1}| = |P|$ also $gPg^{-1} \in Syl_p(G) = P \trianglelefteq G$
b) $\Rightarrow$ a) : Instanz des 2.Sylowsatz $gPg^{-1} = P$. Alle Konjugierten liefern nur $Syl_p(G) = \{P\}$
c) $\Rightarrow$ b) : trivial
a) $\Rightarrow$ c) : Sei $\alpha \in$ Aut G : $\alpha(P) \in Syl_p(G)$

Beispiel :
$|G| = 15 = 3 \cdot 5 \Rightarrow \exists P_3 \in Syl_3(G), \exists P_5 \in Syl_5(G). |Syl_3(G)| \in \{1, 5\}$ und $\equiv 1 \, mod \, 3$. D.h. es bleibt hier nur noch die Wahl $|Syl_3(G)| = 1$ und somit $P_3 \trianglelefteq G$. Auch bei $|Syl_5(G)| \in \{1, 3\}$ und $\equiv 1$ mod 5 bleibt nur die 1, also $P_5 \trianglelefteq G$. Außerdem $P_3 \cap P_5 = \{1\} \Rightarrow G = P_3 \times P_5$ bzw. $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$

Korollar 2 :
Für eine endliche Gruppe sind äquivalent :
a) G ist direktes Produkt der Sylowgruppen
b) alle Sylowgruppen $S \trianglelefteq G \, (\forall p \,|\, |G| \, : |Syl_p(G)| = 1)$

Beweis :
Es sei $|G| = p^{n_1} \cdots p^{n_r}$ mit $p_i \neq p_j$ für $i \neq j$ und $P_i \in Syl_{p_i}(G)$. b) $\Rightarrow$ a) : Nach Voraussetzung ist $P_i \trianglelefteq G$ und $P_i \cap P_1 \cdots P_{i-1} \cdot P_{i+1} \cdots P_r = \{1\} \Rightarrow G = P_1 \times \cdots \times$

Definition :
Ist G endliche Gruppe und Produkt seiner Sylowgruppen, so heißt G **nilpotent**. Eine abelsche Gruppe ist nilpotent.

Beispiel :
$|G| = 56 = 7 \cdot 8$, Behauptung : G hat einen Normalteiler der Ordnung 7 oder 8
$|Syl_7(G)| \mid 8 \equiv 1 mod 7$, d.h. $|Syl_7(G)| \in \{1, 2, 4, 8\} - \{2, 4\}$
1. Fall $|Syl_7(G)| = 1 \Rightarrow \exists P_7 \in Syl_7(G) = \{P_7\}$, $P_7 \trianglelefteq G$
2. Fall $|Syl_7(G)| = 8$ so $P_7 \ntrianglelefteq G$. Dann gibt es 8 Untergruppen der Ordnung 7 mit paarweisen Durchschnitten gleich $\{1\}$. Es gibt $\varphi(7) = 6$ Elemente der Ordnung 7 , also $8 \cdot \varphi(7) = 8 \cdot 6 = 56 - 8$ Es gibt genau 8 Elemente der Ordnung $\neq 7$. Nun gibt es genau eine 2-Sylowgruppe P_2 mit $|P_2| = 8$ und $\{P_2\} = Syl_2(G)$ also $P_2 \trianglelefteq G$.□

1.15 Endliche abelsche Gruppen

18. Vorlesung vom 29.11.2000

Satz 1 :
a) Jede endliche abelsche Gruppe ist direktes Produkt ihrer Sylowgruppen.
b) Zwei endliche abelsche Gruppen sind genau dann isomorph wenn ihre Sylowgruppen paarweise isomorph sind.

Beweis :
zu a) :
Jede Untergruppe ist Normalteiler, also auch alle Sylowgruppen , deshalb gilt nach §1.14 Korollar 2 die Behauptung a) .
zu b) :
Ist $\varphi : G \to H$ ein Isomorphismus, dann $P \in Syl_p(G) \Rightarrow \varphi(P) \in Syl_p(H)$, also $P_i \cong Q_i \Rightarrow P_1 \times \cdots \times P_r \cong Q_1 \times \cdots \times Q_r$.□

Satz 2 :
Ist G abelsche p-Gruppe mit $|G| = p^n$ und $z \in G$ ein Element mit maximaler Ordnung, so ist $G = \langle z \rangle \times U$, $U \leq G$

Beweis :
$\mathbb{M} = \{U \leq G | U \cap \langle z \rangle = \{1\}\} \neq \emptyset \ni \{1\}$
Sei $U \in \mathbb{M}$ maximal bezüglich " $\subseteq$ ", so setzt $W = \langle z \rangle \cap U$. Zu zeigen ist nun, daß $W = G$.
Angenommen $W \subset G$, so existiert $g \in G - W : \sigma(gW)$ also $g^{p^k} \in W$. Wir schreiben g^{p^k} als $z^{ip^l}u$ mit $u \in U$ und $p \not| i$. Dann ist o.B.d.A. i = 1 , sonst ersetzen wir z^i durch z , wegen $\langle z \rangle = \langle z^i \rangle$.
also $g^{p^k} = z^{p^l}u = \sigma(g^{p^k}) = \frac{\sigma(g)}{p^k} = \sigma(z^{p^l}u) \geq \sigma(z^{p^l}) = \frac{z}{p^l}$. Wegen der Maximalität von $\sigma(z)$ folgt $l \geq k$. Dann $g_1 = gz^{-p^{l-k}}$, d.h. $g_1 W = gW$.
$U_1 = \langle g_1 \rangle U$ und $g_1 \in U \subset \langle g_1 \rangle U$, sogar $g_1 \in G - W$.

Behauptung :
$U_1 \cap \langle z \rangle = \{1\}$, demnach ist $U_1 \in \mathbb{M}, U_1 > U$, was ein Widerspruch zur Maximalität von U.

Beweis :
Sei $x \in U_1 \cap \langle z \rangle$, d.h. $\exists j \in \mathbb{N}, v \in U : x = g_1^j v \in \langle z \rangle$, da nun $(\underbrace{g_1 W}_{gW})^j = 1W$ also $j = (g_1 W) \cdot m = p^k m$ mit $m \in \mathbb{Z}$ ist, folgt
daß $x = g^{p^k m} z^{-p^l m} v = (g^{p^k} z^{-p^l})^m v = \underbrace{u^m}_{\in U} \underbrace{v}_{\in U} \in U \cap \langle z \rangle = \{1\} \Rightarrow U_1 \cap \langle z \rangle = \{1\}$,was ein Widerspruch zur Annahme ist.□

Hauptsatz über endlich abelsche Gruppen :
a) Ist G endliche abelsche p-Gruppe, so ist $G \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_r}}$, wobei $n_1 \geq \ldots \geq n_r \in \mathbb{N}$ eindeutig durch G bestimmt sind.
b) Ist G endliche abelsche Gruppe, dann ist $G \cong \mathbb{Z}_{m_1} \dot{\times} \cdots \dot{\times} \mathbb{Z}_{m_t}$ mit $m_i \nmid m_{i-1}$ eindeutig durch G bestimmt.

Beweis :
zu a) : Wende Satz 2 an und eine Induktion, so $G \cong \mathbb{Z}_{p^{n_1}} \times U$ und p^{n_1} die maximale Ordnung eines Elementes $z_1 \in G$ ist. Und weiter ist $G \cong \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times H$, wobei p^{n_2} die maximale Ordnung eines Elementes in $G/\langle z_1 \rangle$ ist, usw.□
zu b) : Wende abermals Satz 2 an und so ist $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_r}} \cong \mathbb{Z}_{p_1^{m_1} p_2^{m_2}}$, falls ggt $(p_1, p_2) = 1$

Beispiel :
$|G| = 24 = 2^3 \cdot 3$ und G abelsch, so existieren die folgenden drei Isomorphietypen :
$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
oder $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$
oder $G \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \cong \mathbb{Z}_{24}$

1.16 Kompositionsreihen

Definition :
a) Eine Ω-Gruppe G heißt **Ω-einfach**, wenn sie genau 2 Ω-Normalteiler, nämlich {1} und G hat (D.h. G = {1} ist nicht einfach).
b) Ist (*) $G = G_0 \trianglerighteq_\Omega G_1 \trianglerighteq_\Omega \ldots \trianglerighteq_\Omega G_n = \{1\}$ Kette von Ω-Untergruppen (bzw. Ω-Normalteilern) von G mit $G_i \trianglelefteq_\Omega G_{i-1}$, so heißt (*) **Ω-Subnormalreihe** (bzw. **Ω-Normalreihe**)
c) Eine **Ω-Kompositionsreihe**, wenn G_{i-1}/G_i Ω-einfach ist. D.h. $G_{i-1} \trianglerighteq_\Omega N \trianglerighteq_\Omega G_i \Rightarrow N \in \{G_{i-1}, G_i\}$
d) (*) heißt **Ω-Hauptreihe**, wenn stets $G_{i-1} \trianglerighteq_\Omega N \trianglerighteq_\Omega G_i$ und $N \trianglelefteq_\Omega G \Rightarrow N \in \{G_{i-1}, G_i\}$
Die Faktorgruppen G_{i-1}/G_i heißen dann **Kompositions-** bzw. **Hauptfaktoren**.

Beispiel :
a) $G \cong (\mathbb{Z}_{12}, +)$ Die Kompositionsreihen sind dann :
$\langle g \rangle \geq \langle g^2 \rangle \geq \langle g^4 \rangle \geq \langle g^{12} \rangle$
$\langle g \rangle \geq \langle g^2 \rangle \geq \langle g^6 \rangle \geq \langle g^{12} \rangle$
$\langle g \rangle \geq \langle g^3 \rangle \geq \langle g^6 \rangle \geq \langle g^{12} \rangle$
Mit den Kompositionsfaktoren :
$\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$
$\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_3$
$\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$

19. Vorlesung vom 1.12.2000

Beispiel :
$G = S_4 \rhd A_4 \rhd V_4 \rhd \langle (12)(34) \rangle \rhd \{1\}$ bzw.
$G = S_4 \rhd A_4 \rhd V_4 \rhd \langle (13)(24) \rangle \rhd \{1\}$ bzw.
$G = S_4 \rhd A_4 \rhd V_4 \rhd \langle (14)(23) \rangle \rhd \{1\}$
Sind Kompositionsreihen mit "Faktoren" :
$S_4/A_4 \cong \mathbb{Z}_2$, $A_4/V_4 \cong \mathbb{Z}_3$, $V_4/\langle (12)(34) \rangle \cong \mathbb{Z}_2$, $\langle (12)(34) \rangle/\{1\} \cong \mathbb{Z}_2$
$G = S_4 \rhd A_4 \rhd V_4 \rhd \{1\}$ ist dann die Hauptreihe.

Definition :
a) Zwei Ω−Subnormalreihen heißen **äquivalent** , wenn die Mengen $\{G_0/G_1, \ldots, G_{n-1}/G_n\} \doteq \{H_0/H_1, \ldots, H_{m-1}/H_m\}$ bis auf Isomorphie gleich sind und n=m gilt. D.h. 1) m=n und 2) $\exists \sigma \in S_n : G_{i-1}/G_i \cong H_{\sigma(i)-1}/H_{\sigma(i)}$
b) Seien (*) $G = G_0 \trianglerighteq_\Omega G_1 \trianglerighteq_\Omega \ldots \trianglerighteq_\Omega G_n = \{1\}$
(**) (*) $H = H_0 \trianglerighteq_\Omega H_1 \trianglerighteq_\Omega \ldots \trianglerighteq_\Omega H_m = \{1\}$,
so heißt (**) Verfeinerung von (*), wenn $\{H_0, H_1, \ldots, H_m\} \supseteq \{G_0, G_1, \ldots, G_n\}$

Butterfly Lemma von Zassenhaussen :
Seien $G_{i+1} \trianglelefteq_\Omega G_i \leq G$ und $H_{j+1} \trianglelefteq_\Omega H_j \leq G$, dann gilt
a) $G_{i+1}(G_i \cap H_{j+1}) \trianglelefteq G_{i+1}(G_i \cap H_j) = G_{ij}$
b) $H_{j+1}(G_i \cap H_j) \trianglelefteq H_{j+1}(G_i \cap H_j) = H_{ij}$
c) $G_{ij}/G_{ij+1} \cong H_{ij}/H_{i+1j}$

Beweis :
Wir wenden den 1. Isomorphiesatz an, der besagt, daß wenn $N \trianglelefteq G$ und $U \leq G$ gilt, $NU \leq G$, $N \cap U \trianglelefteq U$ und $NU/N \cong U/N \cap U$ ist für $G \to G_i$, $N \to G_{i+1}$ und $U \to G_i \cap H_j$. Dann $NU = G_{ij}$ und $N \cap U = G_{i+1} \cap G_i \cap H_j = G_{i+1} \cap H_j \trianglelefteq G_i \cap H_j$ und $G_{ij}/G_{i+1} \cong G_i \cap H_j/G_{i+1} \cap H_j$ mittels des Isomorphismus $\varphi : G_i \cap H_j/G_{i+1} \to G_{ij}/G_{i+1}$, $x(G_{i+1} \cap H_j) \mapsto xG_{i+1}$.
Ebenso ist $G_i \cap H_{j+1} \trianglelefteq G_i \cap H_j$,
$(G_{i+1} \cap H_j)(G_i \cap H_{j+1}) \trianglelefteq G_i \cap H_j$,
$(G_{i+1} \cap H_j)(G_i \cap H_{j+1})/(G_{i+1} \cap H_j) \trianglelefteq (G_i \cap H_j)/(G_{i+1}/H_j)$. So folgt
$\varphi((G_{i+1} \cap H_j)(G_i \cap H_{j+1})/(G_{i+1} \cap H_j)) \trianglelefteq G_{ij}/G_{i+1j}$. Nach dem 2.Isomorphiesatz ist also $G_{ij}/G_{ij+1} \cong G_i \cap H_j/(G_{i+1}H_j)(G_i \cap H_{j+1})$ und genauso $H_{ij}/H_{i+1j} \cong H_j \cap H_j/(G_{i+1}H_j)(G_i \cap H_{j+1})$.□

Verfeinerungssatz von Schreier :
Je 2 Ω-Subnormalreihen von G haben äquivalente Verfeinerungen.

Beweis :
Sei also $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{1\}$ und $G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = \{1\}$ die beiden Subnormalreihen von G.
So definiere $G_{ij} := G_{i+1}(G_i \cap H_j)$ bzw. $H_{ij} := H_{j+1}(G_i \cap H_j)$, so ist $G_i = G_{i0} \trianglerighteq_\Omega G_{i1} \trianglerighteq_\Omega \ldots \trianglerighteq_\Omega G_{im} = G_{i+1}$ und $H_j = H_{0j} \trianglerighteq_\Omega H_{1j} \trianglerighteq_\Omega \ldots \trianglerighteq_\Omega H_{nj} = H_{j+1}$, wobei die (G_{ij}) (bzw. (H_{ij})) Verfeinerungen von (G_i) (bzw. (H_j)) sind.
Nach dem Butterflylemma ist $G_{ij}/G_{ij+1} \cong H_{ij}/H_{i+1j}$, also sind (G_{ij}) und (H_{ij}) äquivalent.

Satz von Jordan , Hölder :
Hat eine Ω -Gruppe eine Kompositionsreihe, so sind je 2 Kompositionsreihen äquivalent. Insbesondere sind je 2 Kompositionsreihen (Hauptreihen) einer endlichen Gruppe äquivalent.

Beispiel :
$(\mathbb{Z}, +)$ hat keine Kompositionsreihe , da $\mathbb{Z} > p\mathbb{Z} > p^2\mathbb{Z} > \ldots$ eine unendliche absteigende Subnormalreihe ist .

1.17 Auflösbare Gruppen

20. Vorlesung vom 4.12.2000

Definition :
Ist G Gruppe und a,b Elemente aus G, so heißt $[a, b] = a^{-1}b^{-1}ab$ **Kommutator**. Und $G' := [G, G] = \langle\, [a, b] | a, b \in G \,\rangle$ (beachte das $\{[a, b] | a, b \in G\}$ im allgemeinen keine Untergruppe ist).

Bemerkung :
$ba[a, b] = ab$

Satz :
a) G' char G (sogar: $\varphi : G \to H$ Epimorphismus $\Rightarrow \varphi(G') = H'$)
b) G ist abelsch $\Leftrightarrow G' = \{1\}$
c) $N \trianglelefteq G$, dann ist G/N abelsch $\Leftrightarrow G' \leq N$, also $G' = \bigcup_{N \trianglelefteq G} N$ ist kleinster Normalteiler mit abelscher Faktorgruppe

Beweis :
zu a) $\varphi([a, b]) = \varphi(a^{-1}b^{-1}ab) = \varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b) = [\varphi(a), \varphi(b)]$
zu b) beachte b) ist Spezialfall von c) für $N = \{1\}$
zu c) Sei G/N abelsch $\Leftrightarrow \forall a, b \in G : (aN)(bN) = (bN)(aN)$, da zwei Nebenklassen aN, bN genau dann gleich sind wenn $a^{-1}b \in N$ ist, dies ist äquivalent zu $(ba)^{-1}ab \in N \Leftrightarrow [a, b] \in N \Leftrightarrow G' \leq N$

Definition :
G sei eine beliebige Gruppe und $G^{(i)} := (G^{(i-1)})'$. G heißt **auflösbar**, wenn $\exists m \in \mathbb{N} : G^{(m)} = \{1\}$. Das kleinste $m \in \mathbb{N}$ mit dieser Eigenschaft heißt **Stufe** von G.
Es gilt : G abelsch $\Leftrightarrow G' = \{1\} \Leftrightarrow$ G auflösbar der 1. Stufe

Beispiel :
$S_3 > S_3' = A_3 > S_3'' = A_3' = \{1\}$ bedeutet, daß die S_3 auflösbar von 2-ter Stufe ist.
bzw. die S_4 ist auflösbar von 3-ter Stufe wegen $S_4 > \underbrace{A_4}_{=S_4'} > \underbrace{V_4}_{=S_4''} > \underbrace{\{1\}}_{=S_4'''}$.
Allerdings sind für $n \geq 5 \in \mathbb{N}$ die S_n nicht auflösbar, da sie alle die nicht auflösbare Untergruppe A_5 enthalten.

Satz 2 :
a) G ist auflösbar $\Leftrightarrow$ G hat eine Subnormalreihe mit abelschen Faktoren
b) G ist endlich und auflösbar $\Leftrightarrow$ G hat eine Kompositionsreihe mit zyklischen Kompositionsfaktoren von Primzahlordnung

Beweis :
zu a) $\Rightarrow$: So ist $G = G' \trianglerighteq G'' \trianglerighteq \ldots \trianglerighteq G^{(m)} = \{1\}$ die (Sub-)Normalreihe mit abelschen Faktoren $G^{(i-1)}/(G^{(i-1)})'$
zu $\Leftarrow$: Sei also $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = \{1\}$ die Subnormalreihe mit abelschen Faktoren, wir behaupten $G^{(i)} \subseteq G_i$.
Induktion: i = 1 : G_0/G_1 abelsch also $G' \leq G_1$ nach Satz 1 c).
Sei $i > 1$: die Induktionsannahme ist, daß $G^{(i-1)} \subseteq G_{i-1}$, es folgt $\underbrace{(G^{(i-1)})'}_{=G^{(i)}} \subseteq \underbrace{G_{i-1}}_{\subseteq G_i}$, wobei G_{i-1}/G_i abelsch ist. Es folgt, daß stets $G^{(i)} \subseteq G_i$ und $G^{(r)} \subseteq G_r = \{1\}$ ist .$\square$
zu b) $\Leftarrow$: gilt nach a)
zu $\Rightarrow$: (*) $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$ ist Kompositionsreihe von G und (**) $G = G' \trianglerighteq G'' \trianglerighteq \ldots \trianglerighteq G^{(m)} = \{1\}$. Nach dem Verfeinerungssatz von Schreier haben (*) und (**) äquivalente Verfeinerungen. D.h. (*) ist eine Verfeinerung von (**), also sind alle Faktoren in (*) abelsch (und einfach) und demnach von zyklisch von Primzahlordnung.

Satz 3 :
a) G ist auflösbar mit $U \leq G$, so auch U auflösbar. Oder anders formuliert besitzt G eine nicht auflösbare Untergruppe U, so ist G selbst auch nicht auflösbar.
b) Sei $N \trianglelefteq G$, dann gilt : G auflösbar $\Leftrightarrow$ N und G/N auflösbar. Insbesondere sind homomorphe Bilder auflösbarer Gruppen, auch auflösbar.

Beweis :
zu a) : Es ist $U' \subseteq G'$ bzw. allg. $U^{(i)} \subseteq G^{(i)}$, also $G^{(m)} = \{1\} \Rightarrow U^{(m)} = \{1\}$
zu b) $\Rightarrow$: $\pi : G \to G/N$ der kanonische Epimorphismus nach Satz 1 und Induktion ist $\pi(G^{(i)}) = (G/N)^i$.
Schließlich ist dann auch $G^{(m)} = \{1\} \Rightarrow (G/N)^{(m)} = \{1\}$, und somit (G/N) ist wie N (nach a))auflösbar .
zu $\Leftarrow$: Sei $N^{(n)} = \{1\}$ und $(G/N)^{(m)} = \{1\} \Leftrightarrow G^{(m)} \leq N$. Also $(G^{(m)})^{(n)} \leq N^{(n)} = \{1\} \Rightarrow G^{(m+n)} = \{1\}$. Die Gruppe G ist auflösbar mit einer Stufe $s \leq m + n$.$\square$

Satz 4 :
Ist G endliche p-Gruppe, so ist G auflösbar.

Beweis :
Es gilt $G \neq \{1\} \Rightarrow$ Z(G)$\neq \{1\}$ (siehe §1.5). Da G auf sich selbst durch Konjugation operiert, wobei die Bahnlängen alle p-Potenzen sind, folgt da $\{1\}$ eine Bahn der Länge $1 = p^0$ ist, daß es mindestens p-1 weitere Bahnen der Länge 1 gibt, daß also mindestens p Element in Z(G) liegen. Da $(Z(G))' = \{1\}$ ist, ist Z(G) abelsch und damit auflösbar. Und G/Z(G) ist wie G eine p-Gruppe mit $|G/Z(G)| < |G|$. Mit Induktion erhält man, daß auch $G/Z(G)$ auflösbar ist, da irgendwann (wegen $|G| < \infty$) $G^{(m)}/Z(G^{(m)}) = \{1\}$ ist, wenn $G^{(i+1)} := G^{(i)}/Z(G^{(i)})$ ist. Nach Satz 3 b) folgt, daß damit auch G auflösbar ist.

p^aq^b-Satz von Burnside 1904 :
Seien p, q Primzahlen und $|G| = p^aq^b$ mit $a, b \in \mathbb{N}$, dann ist G auflösbar.

Beweis :
siehe Vorlesung über Darstellungstheorie

Satz von Feit Thompson 1963 :
Ist $|G|$ ungerade $\Rightarrow$ G auflösbar.

Beweis :
Der Beweis umfasst circa 270 Seiten.

1.18 Einfache Gruppen

Definition :
G **einfach** $\Leftrightarrow$ G hat genau 2 Normalteiler nämlich $\{1\}$ und G $\Leftrightarrow$ G hat keinen echten Normalteiler.

Beispiel :
$G = A_5$ ist einfach (also nicht auflösbar) $\Rightarrow \forall n \in \mathbb{N} : n > 4 \Rightarrow S_n, A_n$ sind nicht auflösbar, da sie A_5 enthalten.

21. Vorlesung vom 6.12.2000

Eine endliche Gruppe G ist genau dann abelsch und einfach, wenn G zyklisch mit Primzahlordnung ist, d.h. $G \cong (\mathbb{Z}/p\mathbb{Z}, \cdot)$ für eine Primzahl.

Beispiel :
Die alternierende Gruppe A_5 ist einfach.

Beweis :
Es ist zu zeigen : $N \trianglelefteq A_5 \Rightarrow N \in \{A_5, \{1\}\}$ ($\Leftrightarrow A_5$ ist einfach).
Sei N ein Normalteiler in A_5, dann ist N die Vereinigung von Konjugiertenklassen, deren Längen 1, 12, 12, 15, 20 sind. Es gilt $1 \in N$, d.h. $|N| \in \{1, 13, 16, 21, 25, 28, 33, \ldots, 60\}$. Wegen $|N| \mid |A_5| = \frac{5!}{2} = 60$, gilt $|N| \in \{1, 60\}$.$\square$

Definition :
G operiere auf X. G operiert **k-fach transitiv**, wenn $|\{x_1, \ldots, x_k\}| = |\{y_1, \ldots, y_k\}| = k$ und $x_i, y_i \in X \Rightarrow \exists g \in G : g \cdot x_i = y_i$ mit $1 \leq i \leq n$.
Es ist offensichtlich, daß die k-fach Transitivität k-1-fach Transitivität impliziert.

Beispiel :
a) S_n ist n-fach transitiv auf $\{1, \ldots, n\}$

b) A_n ist (n-2)-fach transitiv auf $\{1,\dots,n\}$

Beweis :
Sei $\{x_1,\dots x_n\}=\{y_1,\dots,y_n\}=\{1,\dots,n\}$, so existiert ein $\sigma\in S_n$ mit $\sigma\cdot x_i=y_i$ für i=1,…,n.
Dann ist entweder $\sigma\in A_n$ mit $\sigma\cdot x_i=y_i$ für $i=1,\dots,n-2$
oder $\tau\cdot\sigma\in A_n$ mit $\tau=(n-1,n)$ und $\tau\cdot\sigma\cdot x_i=y_i$ für $i=1,\dots,n-2$

Lemma 1 :
Ist $N\trianglelefteq G$ und operiert G mindestens 2-fach transitiv auf X, so operiert N transitiv oder trivial auf X für $|X|<\infty$.
In dem Fall, daß N transitiv auf X operiert gilt : $x\in X\Rightarrow G=N\cdot\mathrm{Stab}_G(x)$

Beweis :
Wir zerlegen X in N Bahnen, also $X=N\cdot x_1\uplus\cdots\uplus N\cdot x_r$. Es ist $(gN)x_i=(Ng)x_i=N(gx_i)\in\{N\cdot x_i|1\le i\le n\}$ und N operiert trivial $\Leftrightarrow Nx_i=\{x_i\}$
Sonst wähle $x_1'\neq x_1\in Nx_i$, dann ist für jedes $g\in G:\{gx_1,gx_1'\}\subseteq N(gx_i)$
Ist $r>1$, d.h. N ist nicht transitiv, so wähle $y_1=x_1$ und $y_2=x_i$ mit $i\neq 1$, dann gibt es kein $g\in G$ mit $gx_1=y_1$ und $gx_1'=gx_i=y_2$.
Sei weiter N transitiv auf X und $x\in X$, d.h. $N\cdot x=X$, so ist
$|X|=[N:Stab_N(x)]=[G:Stab_G(x)]\ge[\underbrace{N\cdot Stab_G(x)}_{\le G}:Stab_G(x)]=[N:Stab_N(x)]=|X|\Rightarrow N\cdot Stab_G(x)=G.\square$

Satz 1 :
Für $n\ge 5$ ist A_n einfach.

Beweis :
Induktionsanfang : siehe Beispiel 1 Induktionsschritt : Sei n > 5, dann ist $G=A_n$ 4-fach transitiv auf $X=\{1,\dots n\}$. Sei $\{1\}\neq N\trianglelefteq G$, so operiert N nicht trivial, d.h. nach Lemma 1 operiert N dann transitiv auf $G=N\cdot\underbrace{Stab_G(n)}_{=A_{n-1}}$, also $G=N\cdot A_{n-1}$. A_{n-1} ist übrigens nach Induktionsannahme einfach.
Betrachte $N\cap A_{n-1}\trianglelefteq A_{n-1}$.
1. Fall : $N\cap A_{n-1}=A_{n-1}$, d.h. $A_{n-1}\le N$, also folgt $N=G$.
2. Fall : $N\cap A_{n-1}=\{1\}$, wegen $N/\{1\}\cong A_n/A_{n-1}$ folgt $|N|=n$. Also gibt zu jedem $i\in\{1,\dots,n\}$ genau ein $h_i\in N$ mit $h_i(n)=i$, denn N operiert transitiv.
Ist $g\in A_{n-1}$, betrachte $gh_ig^{-1}(n)=gh_i(n)=g(i)=h_{g(i)}(n)\in\{1,\dots,n-1\}$. So wähle nun h_i,h_j,h_k,h_l paarweise verschieden, so daß $h_i\cdot h_j=h_k$ und $\{i,j,k,l\}\subseteq\{1,\dots,n-1\}$. Dies ist immer möglich, weil $n=|N|\ge 5$.
A_{n-1} operiert n-3-fach also mindestens 3-fach transitiv auf $\{1,\dots,n-1\}$. Es gibt demnach ein $g\in A_{n-1}$ mit $g(i)=i,g(j)=j,g(k)=l$ und $|\{i,j,k\}|=3=|\{i,j,l\}|$. Somit kann man schließen, daß $gh_ih_jg^{-1}=gh_kg^{-1}=h_{g(k)}=h_l$, aber auch $gh_ih_jg^{-1}=gh_ig^{-1}gh_jg^{-1}=h_{g(i)}h_{g(j)}=h_ih_j=h_k$, wodurch wir einen Widerspruch zu $l\neq k$ erhalten.$\square$

22. Vorlesung vom 6.12.2000

Beispiel :
Ist $\mathrm{SL}(n,\mathbb{F}_p)\trianglelefteq\mathrm{GL}(n,\mathbb{F}_p)$ und $\mathrm{Z}(\mathrm{GL}(n,\mathbb{F}_p))=\{aE_n|a\in\mathbb{F}_p\setminus\{0\}\}$.
Nach Satz 2 ist $\mathrm{SL}(n,\mathbb{F}_p)/\mathrm{Z}(\mathrm{GL}(n,\mathbb{F}_p))=\mathrm{PSL}(n,\mathbb{F}_p)$ ist einfach für $(n,q)\neq(2,2)$ und $(n,q)\neq(2,3)$. Weiter gilt $|\mathrm{GL}(n,\mathbb{F}_p)|=(2^2-1)(2^2-2^1)=6$, $PSL(2,2)=GL(2,2)\cong S_3$, $|GL(2,3)|=(3^2-1)(3^2-3)=48$ und PSL(2,3)$\cong A_4$.

Klassifikation der endlichen einfachen Gruppen :
Ist G eine endliche einfache Gruppe, so ist
i) G abelsch, dann $G\cong(\mathbb{Z}_p,+)$ oder
ii) $G\cong A_n$ mit $n\ge 5$ oder
iii) G ist eine Gruppe vom Typ wie z.B. PSL(n, q) mit (n, q)≠(2,2), (2,3) d.h. G ist eine orthogonale, symplektische Gruppe oder
iv) G ist sporadisch einfach, d.h. eine von 26 Ausnahmegruppen wie z.B. die Monstergruppe M mit $|M|=2^{46}\cdot3^{20}\cdot5^9\cdot7^6\cdot11^2\cdot13^2\cdot17\cdot19\cdot23\cdot29\cdot31\cdot41\cdot47\cdot59\cdot71\approx10^{56}$
Der dazu gehörige Beweis umfaßt mehr als 10000 Seite und wurde ≈ 1981 komplettiert.

Kapitel 2

Ringe

2.1 Ringe und Ideale

Definition :
$(R, +, \cdot)$ heißt **Ring**, wenn
a) $(R, +)$ ist abelsche Gruppe
b) $(R, \cdot)$ ist Monoid (also $\cdot$ ist assoziativ)
c) $\forall a, b, c \in R : (a + b) \cdot c = a \cdot c + b \cdot c$

Bemerkung :
Vielfach wird nur verlangt, daß in Teil b) $(R, \cdot)$ eine Halbgruppe, wir betrachten Ringe als Ringe mit einer Eins.

Definition :
gilt neben a), b), c) zusätzlich, daß
$(R, \cdot)$ ein kommutatives Monoid ist, so heißt $(R, +, \cdot)$ **kommutativer Ring**,
bzw. ist $(R \setminus \{0\}, \cdot)$ eine Gruppe, so heißt R **Divisionsring** oder **Schiefkörper**.
Und falls $(R \setminus \{0\}, \cdot)$ abelsche Gruppe, so ist R ein **Körper** .

Beispiel :
a) $(\mathbb{Z}, +, \cdot)$ ist eine kommutativer Ring
b) $(\mathbb{K}^{n \times n})$ ist für $n > 1$ und K Körper ein nicht kommutativer Ring
c) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_p$ sind Körper

Definition :
Sind $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe, so heißt $\varphi : R \to S$ **Ringhomomorphismus**, wenn
a) $\forall a, b \in R : \varphi(a + b) = \varphi(a) + \varphi(b)$
b) $\forall a, b \in R : \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
c) $\varphi(1_R) = 1_S$
Ist φ zusätzlich bijektiv, so heißt φ **Ringisomorphismus** und $R \cong S \Leftrightarrow \exists \varphi : R \to S$ mit φ ist eine Ringisomorphismus.

Definition :
Ist $\varphi : R \to S$ ein Ringhomomorphismus, so sei **Kern** $\varphi = \{a \in R \,|\, \varphi(a) = 0\} \leq (R, +)$
Es gilt $a \in$Kern $\varphi, x \in R \Rightarrow \varphi(x \cdot a) = \varphi(x) \cdot \varphi(a) = \varphi(x) \cdot 0 = 0$ und $\varphi(a \cdot x) = \varphi(a) \cdot \varphi(x) = 0 \cdot \varphi(x) = 0$.
Folglich sind $a \cdot x$, $x \cdot a \in$ Kern φ.

Definition :
$U \leq R$ heißt **Teilring** von $(R, +, \cdot) \Leftrightarrow 1 \in U, a, b \in U \Rightarrow a \cdot b \in U$ und $(U, +) \leq (R, +)$.
I heißt **Ideal** in $(R, +, \cdot)$, wenn $(I, +) \leq (R, +)$ und $a \in I$, $x \in R \Rightarrow x \cdot a, a \cdot x \in I$.

Homomorphiesatz für Ringe :
a) Sei I ein Ideal in R (kurz $I \trianglelefteq (R, +, \cdot)$). Dann wird $R/I = \{a + I | a \in R\}$ zu einem Ring mit $\cdot : (a + I) \cdot (b + I) = (a \cdot b + I)$ und die Abbildung $\pi = \pi_I : R \to R/I$, $a \mapsto a + I$ ist ein surjektiver Ringhomomorphismus mit $I =$ Kern π.
b) Ist umgekehrt $\Psi : (R, +, \cdot) \to (S, +, \cdot)$ ein Ringhomomorphismus, so ist $I =$ Kern $\Psi \trianglelefteq R$ und es gibt genau einen Ringhomomorphismus $\Psi' : R/I \to S$ mit $\Psi = \Psi' \circ \pi_I$ und $\Psi(a) = \Psi'(a + I)$. Ψ' ist injektiv, also $R/$Kern $\Psi \cong \Psi(R) =$ Bild Ψ. R/I heißt **Restklassenring** nach I .

Beweis :
zu a) Wir zeigen, daß die Multiplikation $\cdot$ wohldefiniert ist. Es gilt $(a + I) = (a' + I), (b + I) = (b' + I) \Leftrightarrow a - a', b - b' \in I$

$\Rightarrow ab - a'b' = a(b-b') + ab' - a'b' = \underbrace{a(\underbrace{b-b'}_{\in I})}_{\in I} + \underbrace{(\underbrace{a-a'}_{\in I})b'}_{\in I}$, weil $I \trianglelefteq R$.
$\Rightarrow ab + I = a'b' + I$. Zudem ist $\cdot$ assoziativ und $1 + I$ ist die Eins. Auch die Distributivität überträgt sich von R auf R/I. Der kanonische Epimorphismus $\pi : R \to R/I$ der additiven Gruppe $(R, +)$ ist ein Ringhomomorphismus.
zu b) Der Homomorphiesatz für Gruppen besagt, daß Ψ' wohldefiniert und injektiv ist, wobei für $I = \text{Kern } \Psi \trianglelefteq R\, \Psi'(a+) = \Psi(a)$ ist. Weiterhin gilt, daß $\Psi'((a+I)(b+I)) = \Psi'(ab+I) = \Psi(ab) = \Psi(a)\Psi(b) = \Psi'(a+I)\Psi'(b+I)$ ist. D.h. Ψ' ist sogar ein Ringhomomorphismus.

23. Vorlesung vom 11.12.2000

Bemerkung :
Ist $I \trianglelefteq R$, so ist $1 \in I \Leftrightarrow J = R$.
$\Leftarrow$: ist trivial. $\Rightarrow$: $1 \in I \trianglelefteq R \ni x$, dann ist $x = x \cdot 1 \in \underbrace{I}_{R \subseteq I}$.

1. Isomorphiesatz :
Sei S ein Teilring von R und I ein Ideal in R, so gilt $S \leq R, I \trianglelefteq R \Rightarrow J + I \leq \wedge I \trianglelefteq S + I \wedge I \cap S \trianglelefteq S$.
Zudem ist $S/I \cap S \cong S + I/I$.

Beweis :
Es ist zu zeigen, daß $(S + I, +) \leq (R, +)$.
Seien dazu $a, b \in I, x, y \in S$, so ist $(x + a) \cdot (y + b) = \underbrace{xy}_{\in S} + \underbrace{xb + ay + ab}_{\in I} \in S + I$ und $1 = 1 + 0 \in S + I$.
Also ist $S + I$ Teilring von R. Daß $I \trianglelefteq S + I$ und $J \cap S \trianglelefteq S$ gilt, ist trivial siehe 1.10. Sei $\Phi : S/I \cap S \to S + I/I$ mit $x+(I \cap S) \mapsto x+I$, so ist Φ offensichtlich ein Isomorphismus der additiven Gruppen. Weiter gilt auch, daß $\Phi(\overline{xy}) = \Phi(\overline{x})\Phi(\overline{y})$, wobei $\overline{x} = x + I \cap D$ bzw. $\overline{y} = y + I \cap D$, also Φ ist ein Ringisomorphismus.

Bemerkung :
$I \trianglelefteq (R, +, \cdot) \Leftrightarrow I$ ist $R \times R$ zulässige Untergruppe von $(R, +)$, wobei $(a, b) \star x = a \cdot x \cdot b$ für $a, b, x \in R$.

2. Isomorphiesatz :
Ist I_1 ein Ideal in R, so ist die Abbildung $\Psi : \{I \trianglelefteq R | I_1 \leq I\} \to \{\overline{I} \trianglelefteq R/I_1 | I \text{ Ideal }\}$ ein Verbandsisomorphismus.

Folgerung :
a) Sei $I \trianglelefteq R$ maximal, d.h. $I \neq R$ und $I \leq I' \trianglelefteq R \Rightarrow I = I' \vee I' = R$. Dann ist I ist maximal $\Leftrightarrow R/I$ ist einfach
b) R sei kommutativer Ring, dann gilt R/I ist Körper $\Leftrightarrow I$ ist maximales Ideal in R.
Oder wenn R kommutativ ist, so gilt R ist Körper $\Leftrightarrow$ R ist einfach.

Beweis :
a) klar
b) zu zeigen mit Voraussetzung, daß R kommutativ ist: R Körper $\Leftrightarrow$ R einfach.
zu $\Rightarrow$: Sei R Körper und $\{0\} \neq I \trianglelefteq R$. Wähle $a \in I \setminus \{o\}$. Dann ist $1 = a^{-1} \underbrace{a}_{\in I} \in I$. Wir haben bereits gesehen, daß $1 \in I \Rightarrow I = R$.$\square$.
zu $\Leftarrow$: Sei $0 \neq a \in R$, dann ist zu zeigen: $\exists x = a^{-1} \in R$ mit $1 = x \cdot a$. Es ist $0 \neq a = 1 \cdot a \in \underbrace{Ra}_{\neq\{0\}} \trianglelefteq R$, also Ra ist das von a erzeugte Hauptideal. Da aber R einfach ist, existieren zur die beiden Ideale $\{0\}$ und R. Folglich ist $Ra = R$. Wegen $1 \in R$, folgt $\exists x \in R : x \cdot a = 1$.$\square$

Beispiel :
Sei $m \in \mathbb{N}_0$ und somit $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, dann ist $m\mathbb{Z}$ maximales Ideal $\Leftrightarrow$ m ist Primzahl ($m\mathbb{Z} \leq n\mathbb{Z} \Leftrightarrow n \mid m$).

2.2 Integritätsringe und Quotientenkörper

Voraussetzung :
In diesem Abschnitt ist mit $(R, +, \cdot)$ stets ein kommutativer Ring gemeint.

Definition :
a) R heißt **Integritätsring**, **Integritätsbereich** bzw. **nullteilerfrei**, wenn $\forall a, b \in R : a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ und $0 \neq 1$.
b) $P \trianglelefteq R$ heißt **Primideal**, wenn aus $a, b \in R$ und $a \cdot b \in P \Rightarrow a \in P$ oder $b \in P$.

Behauptung :
a) Ist $I \trianglelefteq R$, dann gilt I ist Primideal $\Leftrightarrow R \setminus I$ ist Integritätsring.
b) $\{0\}$ ist Primideal in R $\Leftrightarrow$ R ist Integritätsring
c) Ist R Teilring eines Körpers, so ist R Integritätsbereich.
d) Sei P ein maximales Ideal in R $\Rightarrow$ P ist Primideal.

Beweis :
a) $R \setminus I$ ist Integritätsbereich $\Leftrightarrow \underbrace{(a+I)(b+I)}_{ab+I} = 0 \Rightarrow a+I = \mathrm{o}+I \vee b+I = \mathrm{o}+I$. Dies gilt logischerweise, da R ein Integritätsbereich ist und damit in R aus $ab = 0$, $a = 0 \vee b = 0$ folgt.
b) klar
c) Ist $R \leq K$ Körper, wegen $R \subseteq K$ ist und da nur die 0 Nullteiler in K ist $\Rightarrow$ R ist Integritätsring.
d) P maximales Ideal $\Rightarrow R \setminus P$ ist Körper und erst recht Integritätsring $\overset{\Rightarrow}{a)}$ P Primideal

Satz 1 :
R sei Integritätsring und H eine Teilmenge mit den folgenden Eigenschaften: $H \cdot H \subseteq H, 1 \in H$ und $0 \notin H$.
z.B. erfüllen $H = R \setminus \{0\}$ und $H = R \setminus P$ diese Bedingungen.
Auf $M = R \times H$ definiere die Relation $(a,b) \sim (c,d) :\Leftrightarrow ad = bc$. Dann ist $\sim$ ein Äquivalenzrelation, wobei die Äquivalenzklasse von (a,b) für $a \in R, b \in H$ $\frac{a}{b} = \{(c,d) \in R \times H | (c,d) \sim (a,b)\}$ ist. $Q(R,H) = \{\frac{x}{y} | x \in R, y \in H\}$

Definition :
$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$ und $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.
Damit wird $(Q(R,H), +, \cdot)$ zu einem kommutativen Ring und die Abbildung $\varphi : R \to Q(R,H)$, $a \mapsto \frac{a}{1}$ ist injektiver Ringhomomorphismus und damit wird R zum Teilring. Jedes $h \in H$ hat dann in $Q(R,H)$ ein Inverses $\frac{1}{h}$. Für $H = R \setminus \{0\}$ sagt man Quot R $= Q(R,H)$ ist der **Quotientenkörper** von R.

24. Vorlesung vom 13.12.2000

Beweis zu Satz 1 :
Sei R ein Integritätsring und $H \subseteq R$ mit $H \cdot H \subseteq H$, $1 \in H$ und $0 \notin H$. Auf $R \times H$ ist dann $\sim$ als $(a,b) \sim (c,d) \Leftrightarrow ad = bc$ definiert. zu zeigen $\sim$ ist eine Äquivalenzrelation :
$\sim$ ist reflexiv, denn $(a,b) \sim (a,b)$ wegen $ab = ba$.
$\sim$ ist symmetrisch, da $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$, weil R kommutativ ist.
$\sim$ ist transitiv, denn sei $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$,
so ist $ad = bc$ und $cf = de \Rightarrow (af - be) \underbrace{d}_{\in H \neq 0} = fad - bde = 0 \Rightarrow af = be \Leftrightarrow (a,b) \sim (e,f)$.
Bleibt noch zu zeigen, daß + und $\cdot$ wohldefiniert sind:
zu + : $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$, d.h $ab' = a'b$ und $cd' = c'd$. Zu zeigen : $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$
Es ist $(ad+bc)b'd' = a'bdd' + bb'c'd = (a'd' + b'c')bd.\square$. Die Wohldefiniertheit des $\cdot$ läßt sich ganz analog zeigen.

$(Q(R,H), +)$ ist abelsche Gruppe mit Null $\frac{0}{1}$ und $(Q(R,H), +, \cdot)$ ist kommutativer Ring mit $1 = \frac{1}{1}$. Die Einbettung $R \hookrightarrow Q(R,H)$, $a \mapsto \frac{a}{1}$ ist ein injektiver Ringhomomorphismus. Man identifiert häufig ein Element a in R mit $\frac{a}{1}$ in Q(R,H) , d.h. man betracht $R \subseteq Q(R,H)$. Alle Elemente $a \in H$ haben in Q(R,H) ein Inverses, nämlich $\frac{1}{a} \in Q(R,H)$. Ist $H = R \setminus \{0\}$, so haben alle Elemente $\frac{a}{b}$ in Q(R,H) ein Inverses, nämlich $\frac{b}{a} \in Q(R,H)$. In diesem Fall ist $Q(R, R \setminus \{0\})$ ein Körper, wir nennen ihn den Quotientenkörper Quot(R) von R.

Bemerkung :
Ist R ein Integritätsring und $R \subseteq K$ Körper, so ist die Abbildung $\varphi : Quot(R) \hookrightarrow K$, $\frac{a}{b} \mapsto ab^{-1}$ eine Einbettung, d.h. ein inejktiver Ringhomomorphismus.

Beispiel :
a) Seien $R = \mathbb{Z}, H = \mathbb{Z} \setminus \{0\}$, dann gilt Quot$(\mathbb{Z}) = \mathbb{Q}$.
b) Seien $R = \mathbb{Z}$ und $H = \mathbb{Z} \setminus p\mathbb{Z}$, so ist $Q(R,H) = \{\frac{a}{b} | a \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_{(p)}$ und $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$.
c) Ist $R = K[X]$ mit K ist Körper und X eine Unbestimmte. So ist Quot $K[X] =: K(X) =$ Körper der rationalen Funktionen über K $= \{\frac{f}{g} | f, g \in K[X], g \neq 0\}$.
d) Oder $R = K[X]$ mit K Körper und a $\in$ K, so sei $P := \{f \in K[X] | f(a) = 0\} \trianglelefteq K[X]$. So bezeichnet man Quot$(K[X], K[X] \setminus P) = \{\frac{f}{g} | f, g \in K[X], g(a) \neq 0\} \subseteq K(X)$ die Lokalisierung von $K[X]$ an a.

Zusammenfassung :
Jeder Integritätsring kann in einen Körper eingebettet werden.

2.3 Hauptideale

Voraussetzung :
R sei immer ein Integritätsring.

Definition :
Sei $a \in R$, so heißt $Ra = (a) = \{xa | x \in R\}$ das von a erzeugte **Hauptideal**. Wenn a ,b aus R sind, so gilt $a \mid b \Leftrightarrow \exists x \in R : b = xa$. Wir nennen zwei Element a, b **assoziiert** oder kurz $a \sim b \Leftrightarrow a \mid b \wedge b \mid a$. Und a $\in R$ heißt **Einheit** genau dann, wenn $a \mid 1$ oder anders formuliert a ist in R invertierbar.

Bemerkung :
$a \mid b \Leftrightarrow b \in Ra \Leftrightarrow Rb \subseteq Ra$
a ist zu b assoziiert $\Leftrightarrow Ra = Rb$
a ist ein Einheit $\Leftrightarrow Ra = R \Leftrightarrow a \in R^\star$, wobei $R^\star$ die Einheitengruppe von R ist.

Definition :
Ein Element $q \in R \setminus R^\star$ heißt **irreduzibel** $:\Leftrightarrow \exists a, b \in R : q = a \cdot b \Rightarrow a \in R^\star \vee b \in R^\star$. Und p $\in R \setminus R^\star$ heißt **Primelement** $:\Leftrightarrow p \neq 0 \wedge p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$.

Beispiel :
a) Sei $R = \mathbb{Z}, \mathbb{Z}^\star = \{1, -1\}$. Es gilt $q \in \mathbb{Z}$ ist irreduzibel $\Leftrightarrow q = \pm p$ mit p Primzahl $\Leftrightarrow q$ ist Primelement.
b) Oder sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b \cdot \sqrt{-5} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ und $R^\star = \{1, -1\}$. Hier ist 3 irreduzibel, aber kein Primelement denn es gilt $3 \mid 3^2 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, aber $3 \nmid 2 + \sqrt{-5} \wedge 3 \nmid 2 - \sqrt{-5}$.
Es wäre wünschenwert, wenn in R 3 und $2 + \sqrt{-5}$ ein gemeinsamen Teiler a hätten, so wäre $R3 \subseteq Ra \subseteq R$. Es gilt aber z.B. für das Ideal $I = R3 + R(2 + \sqrt{-5})$, daß $R3 \nsubseteq I \nsubseteq R$ und $R(2 + \sqrt{-5}) \nsubseteq I \nsubseteq R$.

25. Vorlesung vom 15.12.2000

Satz 1 :
a) p Primelement $\Rightarrow$ p ist irreduzibel
b) p Primelement $\Rightarrow (p) = Rp$ ist ein Primideal $P \neq \{0\}$
c) p irreduzibel $\Leftrightarrow Rp \neq R$ und $Rp \subsetneq Ra \trianglelefteq R \Rightarrow Ra = R$, d.h.$Rp$ ist maximal in der Menge der nichttrivialen Hauptideale

Beweis :
zu a) p sei ein Primelement, d.h. $0 \neq p \in P \setminus R^\star$. Da p Primelement ist, gilt $p \mid ab \Rightarrow p \mid a \vee p \mid b$. O.b.d.A. gilt nun $p \mid a$, d.h. $\exists x \in R : a = px$. Deshalb gilt dann auch $p = ab = pxb \Leftrightarrow \underbrace{p}_{\neq 0}(1 - xb) = 0$. Da R ein Integritätsbereich ist, folgt $b \in R^\star$.$\square$
zu b) Sei $P \trianglelefteq R$ ein Primideal. Per Definition gilt : $\underbrace{ab \in P}_{\Leftrightarrow p \mid ab} \Rightarrow \underbrace{a \in P}_{\Leftrightarrow p \mid a} \vee \underbrace{b \in P}_{\Leftrightarrow p \mid b}$. D.h. $P = (p) = Rp$.
zu c) Sei $0 \neq p \notin R^\star \Leftrightarrow Rp \neq R$. So ist $Rp \subsetneq Ra \Leftrightarrow p = ab$ mit $b \notin R^\star$
p ist irreduzibel $\Leftrightarrow p = ab, b \notin R^\star \Rightarrow a \in R^\star$ bzw. $Ra = R$.

Definition :
Ein Integritätsring R heißt **Hauptidealring**, wenn jedes Ideal von R ein Hauptideal ist.

Beispiel :
a) $\mathbb{Z}$ ist ein Hauptidealring
b) K Körper $\Rightarrow$ K Hauptidealring, denn $K^\star = K \setminus \{0\}$ hat keine Primelemente und auch keine irreduzibelen Element.

Satz 2 :
Sei R ein Hauptidealring aber kein Körper, dann gilt :
a) $p \in R$ irreduzibel $\Leftrightarrow$ p Primelement
b) $I \trianglelefteq R$ maximal $\Leftrightarrow \{0\} \neq I$ Primideal in R
c) Sei $\{0\} \neq I \trianglelefteq R$, so ist $R \setminus I$ Integritätsbereich $\Leftrightarrow R \setminus I$ ist Körper, bzw. $I \trianglelefteq R$ maximal $\Leftrightarrow R \setminus I$ ist Körper

Beweis :
zu b) $\Rightarrow$: Anwendung von Satz 1c)
zu $\Leftarrow$: Sei $0 \neq Rp = I$ Primideal, demnach p ist Primelement, also auch irreduzibel. Nach Satz 1c) und der Voraussetzung ist Rp maximal
zu a) $\Leftarrow$: Anwendung von Satz 1a)
zu $\Rightarrow$: Sei p irreduzibel nach Satz 1c) ist Rp ein maximales Ideal in R. d.h. aber nach Satz 1b) daß p Primelement ist.
zu c) Umformulierung von b.$\square$

Definition :
Ein **Euklidischer Ring** ist ein Integritätsring R zu dem es eine Abbildung $\delta : R\ \{0\} \to \mathbb{N}_0$ gibt mit der Eigenschaft zu $a, b \in R$ existieren $q, r \in R$ mit $a = qb + r$ für r = 0 oder $\delta(r) < \delta(b)$.

Beispiel :
a) Die ganzen Zahlen also $\mathbb{Z}$ mit der Abbildung *delta*, wobei $\delta(a) = |a|$
b) Falls K ein Körper ist, so ist $K[X]$ ein Euklidischer Bereich mit $\delta(f) = \delta(\sum_{i=0}^{n} a_i X^i = gradf = n$

Satz 3 :
Ist R Euklidischer Ring, so ist R Hauptidealring.

Beweis :
Sei $\{0\} \neq I \trianglelefteq R$, dann suchen wir ein $d \in R$ mit $I = (d) = Rd$. Wähle $0 \neq d \in I$ mit $\delta(d) = \min\{\delta(a)|a \in I \setminus \{o\}\}$. Da $d \in I$ ist, gilt $Rd \subseteq I$. Sei umgekehrt $0 \neq aI$. Nach Vorraussetzung existieren $q, r \in R$ mit $a = q \cdot d + r$ mit $r = 0$ oder $\delta(r) < \delta(d)$. Da $a, d \in I$ gilt $r = a - q \cdot d \in I$. Für $r = 0$ folgt sofort $a \in Rd$. Wäre $r \neq 0$, so wäre $\delta(d)$ nicht minimal, was einen Widerspruch zur Annahme bedeutet. Also $a \in Rd$.□

Folgerung :
K Körper $\Rightarrow K[X]$ ist Hauptidealring.

Beispiel :
$\mathbb{Z}[X]$ ist kein Hauptidealring.

2.4 Faktorielle Ringe

Definition :
R heißt **faktoriell** (oder **Gaußscher Ring** oder **ZPE-Ring**), wenn R ein Integritätsring ist und
i) zu jedem $0 \neq a \in R \setminus R^\star$ gibt es irreduzibele Element $q_1, \ldots, q_n$ mit $a = q_i \cdots q_n$.
ii) Ist $q_1 \cdots q_n = p_1 \cdots p_m$ $(q_i, p_i irreduzibel)$, so ist m=n und es existiert $\sigma \in S_n$ mit q_i ist assoziert zu $p_{\sigma(i)}$. D.h. $\exists \epsilon_i \in R^\star : q_i = \epsilon_i p_{\sigma(i)}$.

Beispiel :
a) $\mathbb{Z}$ ist faktoriell.
b) $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, wegen $9 = 3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$, aber $3 \nmid 2 + \sqrt{-5}$, d.h. ii) ist verletzt

25. Vorlesung vom 18.12.2000

Satz 1 :
Äquivalent sind für einen Integritätsring R die folgenden Aussagen :
a) R ist faktoriell
b) jedes irreduzibelle Element in R ist Primelement und jedes $0 \neq a \in R \setminus R^\star$ ist Produkt von endlich vielen Primelementen
c) Jedes $0 \neq a \in R \setminus R^\star$ ist Produkt von endlich vielen Primelementen

Beweis :
zu a) $\Rightarrow$ b): Es ist zu zeigen: q irreduzibel $\Rightarrow$ q Primelement, denn $\Leftarrow$ gilt stets in jedem Integritätsring.
Sei $q \mid a \cdot b$, so existiert x ∈ R mit $a \cdot b = q \cdot x$. Nach Voraussetzung i) gibt es irreduzible Element $q_1, \ldots, q_n \in R$ mit $a = q_1 \cdots q_k$ und $b = q_{k+1} \cdots q_n$ und falls $x \notin R^\star$ gibt es q_1' bis q_s' ∈ R (irr.), so daß $q_1 \cdots q_n = q \cdot q_1' \cdots q_s'$ ist. Aus ii) folgt dann $\exists i$: q und q_i sind assoziiert. Also wenn $i \leq k$ ist so $q \mid a$ sonst $q \mid b$.D.h. aber q ist Primelement.
b) $\Rightarrow$ c) ist trivial
zu c) $\Rightarrow$ a) : Da Primelemente irreduzibel sind, gilt i). Bleibt noch ii) zu zeigen. Es sei $q_1 \cdots q_n = p_1 \cdots p_m$, wobei q_i irreduzibel und p_i Primelemente sind. Induktion nach m:
$m = 1 : p_1 \mid q_1(q_2 \cdots q_m) \Rightarrow p_1 \mid q_1$ oder $p_1 \mid q_2 \cdots q_m$. Also $\exists i$ mit $p_1 \mid q_i = p_1 \cdot \epsilon$ mit ϵ Einheit, weil die q_i irreduzibel sind. O.B.d.A ist $i = 1$, somit $p_1 = q_1 \cdots q_n = p_1 \epsilon q_2 \cdots q_n \Rightarrow p_1(1 - \epsilon q_2 \cdots q_n) = 0 \Rightarrow 1 = \epsilon q_2 \cdots q_n$.Das bedeutet es existiert ein $q_j, j > 1$ mit $q_j \in R^\star$. Das geht aber nur für $n = 1$. Demnach ist $p_1 = q_1$, also q_1 Primelement und $n = m$.
$m > 1 : p_1 \cdots q_1 \cdots q_n$ wie oben existiert i mit $p_1 \mid q_i$. O.B.d.A. $p_1 \mid q_i = p_i \epsilon$ mit $\epsilon \in R^\star$ und $p_1 \cdots p_m = p_1 \epsilon q_2 \cdots q_n$. Nach Induktionsannahme ist $m - 1 = n - 1$ und nach Umsortierung ist p_j assoziiert zu q_j für $j = 2 \ldots m$.□

Definition :
Ein kommutativer Ring heißt **noethersch**, wenn jede aufsteigende Kette von Idealen abbricht, d.h. für $i \in \mathbb{N}$ und $I \trianglelefteq R\ I_i \subseteq I_{i+1} \Rightarrow \exists j \in N$ mit $\forall n \in \mathbb{N} : I_j = I_{j+1}$.

Satz 2 :
Jeder Hauptidealring R ist noethersch.

Beweis :
Seien $I_i \trianglelefteq R$ mit $\forall i \in \mathbb{N} : I_i \subseteq I_{i+1}$. Wir zeigen zuerst, daß $I = \bigcup I_i \trianglelefteq R, i \in \mathbb{N}$ ist. Dazu seien $a, b, 0 \in I$, so existieren $i, j \in \mathbb{N}$ mit $a \in I_i, b \in I_j$. Setze $k := \max\{i, j\}$, dann $a, b \in I_k$ und damit auch $a \pm b \in I_k \subseteq I$ und $x \in R \Rightarrow x \cdot a \in I_k \subseteq I$. Also $I \trianglelefteq R$. Da R ein Hauptidealring ist existiert ein Element $d \in R$ mit $I = Rd = (d)$. Wieder existiert ein $i \in \mathbb{N}$ mit $d \in I_i \trianglelefteq R$. Fassen wir also zusammen : $I \subseteq Rd \subseteq I_i \subseteq I_{i+k} \subseteq I$ für alle $k \in \mathbb{N}$, also $\forall k \in \mathbb{N} : I_i = I_{i+k} = I$.$_{Box}$

Satz 3 :
Ist R ein Integritätsring und noethersch, so ist jedes $0 \neq a \in R \setminus R^\star$ ein Produkt von endlich vielen irreduziblen Elementen.

Beweis :
Wir zeigen erst, daß $0 \neq a \in R \setminus R^\star$ hat einen irreduziblen Faktor q hat. Sei dazu $a = q \cdot x$, $x \in R$. Ist jetzt a irreduzibel, so setze $q = a$ und $x = 1$ und die Behauptung gilt. Sonst ist $a = q_1 \cdot q_1'$ mit $q_1, q_1' \in R \setminus (R^\star \cup \{0\}) \Rightarrow Ra \subset Rq_1$. Falls nun q_1 irreduzibel ist sind wir fertig, sonst spalte q_1 in $q_2 \cdot q_2'$ auf mit $0 \neq q_2, q_2' \in R \setminus R^\star$, somit ist wieder $Rq_1 \subset Rq_2$, und so weiter. Da aber R noethersch ist, gibt es keine unendliche Kette von Idealen, d.h. $\exists n \in \mathbb{N}$, sodaß a den irreduziblen Faktor q_n hat und $a = q_1 \cdot q_2 \cdots q_n$ ist. Es bleibt noch zu zeigen, daß a nicht in unendlich vielen irreduzible Faktoren zerfällt. Wir wissen a hat die Form $a = q_1 \cdot a_1$ für $a_1 \in R$ und ein irreduzibles Element q_1. Ist nun $0 \neq a_1 \in R^\star$, dann sind a und q_1 assoziert und demnach a irreduzibel. Sonst hat a_1 wie wir wissen ein irreduziblen Faktor q_2, folglich gilt $Ra \subset Rq_1 \subset Rq_2 \ldots$. R ist aber noethersch, d.h. für ein $n \in \mathbb{N}$ ist $a = q_1 q_2 \cdots q_{n-1} \underbrace{(q_n \cdot a_n)}_{irr.}$, was die Behauptung ist.$\square$

Folgerung :
Jeder Hauptidealring R ist faktoriell.

Beweis :
Da R ein Hauptidealring ist, ist R nach Satz 2 ein noetherscher Integritätsring. Satz 3 besagt nun, daß jedes Element aus R ein Produkt von endlich vielen irreduziblen Elementen ist. Da aber nach §3 Satz 2 in einem Hauptidealring jedes irreduzible Element auch prim, folgt mit Satz 1 R ist faktoriell .$\square$

Bemerkung :
Es gelten die folgenden Relationen für Ring :
$\{R|R$ Körper$\} \subseteq \{R|R$ euklischer Ring$\} \subseteq \{R|R$ Hauptidealring$\} \subseteq \{R|$ faktoriell$\} \subseteq \{R|R$ Integritätsring$\}$

Beispiele :
a) $\mathbb{Z}$ und $K[X]$ (K Körper) sind euklidischer Ringe
b) $\mathbb{Z}[\frac{\sqrt{-163}+1}{2}]$ ist ein Hauptidealring
c) $\mathbb{Z}[X]$ und $K[X, Y]$ (K Körper) sind faktorielle Ringe
d) $\mathbb{Z}[\sqrt{-5}]$ und $\mathbb{Z}[\sqrt{11}]$ sind Integritätsbereiche
Alle diese Beispiele liegen nicht in der spezielleren, übergeordneten Klasse von Ringen.

26. Vorlesung vom 20.12.2000

2.5 Polynomringe über faktoriellen Ringen

Wir nehmen an R sei ein Integritätsbereich und X eine Unbestimmte. Es ist $R \subseteq$Quot $R = K$ und $R[X] \subset K[X]$ wie z.B. für $R = \mathbb{Z}$ und $K = \mathbb{Q}$. Ist nun $f = \sum_{i=0}^{n} a_i X^i$ für $a_i \in K$, so existiert ein Element $0 \neq d \in R$ mit $df \in R[X]$.

Frage :
a) Gilt $df \in R[X]$ irreduzibel in $R[X] \Leftrightarrow f$ irreduzibel in $K[X]$?
b) Ist $R[X]$ faktoriell ?

Voraussetzung :
R sei faktoriell.

Definition :
$f \in R[X]$ heißt **primitiv**, wenn $f = \sum_{i=0}^{n} a_i X^i$ mit $a_n \neq 0$ und $\text{ggt}(a_0, \ldots, a_n) = 1$.

Lemma :
Ist $f \in R[X]$ primitiv und irreduzibel in $K[X]$, so f irreduzibel in $R[X]$.

Beweis :
Ist $f = g \cdot h$ für $g, h \in R[X]$. O.B.d.A. ist grad $g = 0$ bzw. $g \in R$, da f irreduzibel in $K[X]$ ist. Weiterhin ist $g \in R^\star$, weil f

primitiv ist.

Erinnerung :
Sind R, S kommutative Ringe und $\varphi : R \to S$ ein Ringhomomorphismus, so existiert $\hat{\varphi} : R[X] \to S[X]$ definiert durch $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \varphi(a_i) X^i$.

Beispiel :
Sei $P \trianglelefteq R$, z.B. $P = p\mathbb{Z}$ und $R = \mathbb{Z}$. So ist φ der kanonische Epimorphismus $R \to R \setminus P$, der jedem Element a seine Restklasse $\overline{a} = a + R$. Da $R \subset R[X]$ und $R \setminus P \subset R \setminus P[X]$ gilt, ist $\hat{\varphi} : R[X] \to R \setminus P[X]$ die natürliche Fortsetzung von φ mittels $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a_i} X^i$.

Lemma von Gauß :
R sei faktoriell und $P \trianglelefteq R$ ein Ideal in R, so ist
a) P ist Primideal in R $\Leftrightarrow P[X] = \{\sum_{i=0}^{n} a_i X^i | a_i \in P, n \in \mathbb{N}_0\}$ ist ein Primideal in R[X]
b) $f, g \in R[X]$ primitiv $\Rightarrow f \cdot g$ ist primitiv

Beweis :
zu a): P ist Primideal $\Leftrightarrow$ R/P ist Integritätsbereich $\Leftrightarrow$(R/P)$[X] = \hat{\varphi}(R[X])$ ist Integritätsbereich $\overset{\Leftrightarrow}{Hom.satz}$ R[X]/P[X] Integritätsring $\Leftrightarrow P[X]$ ist Primideal in $R[X]$.
zu b) Angenommen f, g seinen nicht primitiv, so existiert $d \in R\mathbb{R}^\star$, wobei d alle Koeffizienten von $f \cdot g$ teilt. Dann exisitert ein Primteiler p von d, da R faktoriell ist, so $p \mid f \cdot g \Rightarrow f \cdot g \in P[X] = (p)[X]$. Nach a) ist P[X] somit auch ein Primideal, da P ein Primideal ist. D.h. $f \in P[X]$ oder $g \in P[X]$ bzw. f oder g ist nicht primitiv. Das ist ein Widerspruch zur Voraussetzung, das f, g primtiv waren, also ist $f \cdot g$ primitiv.

Lemma :
R sei faktoriell, $f \in R[x]$
a) $\tilde{g}, \tilde{h} \in K[X]$ mit $f = \tilde{g}\tilde{h}$, dann existieren $c, c' \in K$ mit $\tilde{g} = cg$ und $\tilde{h} = c'h \in R[X]$ wobei g, h primitiv sind und $f = rgh$ für $r = cc'$.
b) Wenn $f \in R[X]$ mit grad $f > 0$ irreduzibel in $R[X]$ ist $\Rightarrow$ f irreduzibel in $K[X]$

Beweis :
zu a) Falls $\tilde{g} = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i$ und $\tilde{h} = \sum_{i=0}^{n} \frac{a_i'}{b_i'} X^i$ mit $a_i, b_i, a_i', b_i' \in R$ sind, so ist $b\tilde{g} = dg \in R[X]$ und $b'\tilde{h} = d'h \in R[X]$, wobei $d, d' \in R$, $b = \Pi b_i$, $b' = \Pi b_i'$ und g bzw. f primitiv sind. Somit folgt $bb'\tilde{g}\tilde{h} = f = dd'gh$ mit $g \cdot h$ primitiv nach Lemma von Gauß. D.h. aber $bb' \mid dd' = rbb'$ mit $r \in R \Rightarrow f = \frac{dd'}{bb'} gh = rgh$.
zu b) Angenommen f sei in K[X] reduzibel. So ist $f \in R[X]$, grad $f > 0$ und $f = \tilde{g}\tilde{h}$ mit grad f und grad $g > 0$. Nach a) ist aber f existieren $g, h \in R[X]$, sodaß $f = \tilde{g}\tilde{h} = rgh$ mit grad g = grad $\tilde{g} > 0$ und grad h = grad $\tilde{h} > 0$. Demnach sind $g, h \notin R[X]^\star$, womit wir einen Widerspruch zur Irreduzibilität von f in $R[X]$ haben.□

Satz von Gauß :
R faktoriell $\Rightarrow R[X]$ faktoriell

Beweis :
Wir zeigen: a) Jedes irreduzible Element in R[X] ist Primelement und b) Jedes $0 \neq f \in R[X] \setminus R[X]^\star$ ist Produkt von irreduziblen Elementen in R[X].
zu a) Sei $f \in R[X]$ irreduzibel und $f \mid g \cdot h$ mit $g, h \in R[X]$.
1.Fall: grad $f = 0$: Dann ist $f \in R$ und irreduzibel in R, also Primelement in R. Also $f = g \cdot h \in (Rp)[X]$ und mit dem Lemma von Gauß erhalten wir $f \mid g$ oder $f \mid h$.
2.Fall: grad $f > 0$. Da f irreduzibel in R[X] ist, ist es auch in K[X] irreduzibel. Also $f \mid g$ im Hauptidealring K[X] oder $f \mid h$, was auch für R[X] zutrifft.
zu b) Sei $0 \neq f \in R[X] \setminus R[X]^\star$.
1. Fall: grad $f = 0$, so f $\in R \setminus R^\star$ und $f = p_1 \cdots p_m$, da R faktoriell. Die p_i sind aber auch in $R[X]$ irreduzibel, d.h. die Behauptung stimmt.
2. Fall: grad $f > 0$, so ist $f = \tilde{g}_i \cdots \tilde{g}_m$ und $g_i \in K[X]$ sind irreduzibel. So ist auch $f = rg_1 \cdots g_m$ mit $r \in R$ und $g_i \in R[X]$, wobei grad g_i = grad $\tilde{g}_i > 0$. Zerlege noch $r \in R$ in ein Produkt von irreduziblen Element ($r = p_1 \cdots p_n$, so ist $f = p_1 \cdots p_n g_1 \cdots g_m$ das gesuchte Produkt von irreduziblen Elementen .□

27. Vorlesung vom 22.12.2000

Definition :
Der Ring $K[X_1, \ldots, X_n] := K[X_1, \ldots, X_{n-1}][X_n] = \{\sum_{endl.} a_{i_1} \cdots a_{i_n} X^{i_1} \cdot X^{i_n} | a_{i_j} \in K\}$ ist nach dem Satz von Gauß faktoriell. Dann heißt $M \subseteq K^n$ **algebraisch** $\Leftrightarrow$ $f_i \in K[X_1, \ldots, X_n]$ mit $i \in I$ existieren mit der Eigenschaft, daß $M = \{(x_1, \ldots, x_n) \in K^n | f_i(x_1, \ldots, x_n) = 0\} = V(f_i | i \in I)$.

Beispiel :
(affine) Teilräume bzw. Quadriken usw.

Bemerkung Sei $I_M = \{f \in K[X_1, \ldots, X_n] | \forall (x_1, \ldots, x_n) \in M : f(X_1, \ldots, X_n) = 0\}$ ist ein Ideal in $K[X_1, \ldots, X_n]$. Außerdem ist jedes Ideal in $K[X_1, \ldots, X_n]$ endlich erzeigt. Der Basis Satz von Hilbert lautet : R noethersch $\Rightarrow$ R[X] noethersch. An dieser Stelle beginnt die algebraisch Geometrie. Die z.B. sagt, daß $V(f \cdot g) = V(f) \cap V(g)$ ist, dann $f \cdot g(x_1, \ldots, x_n) = 0 \Leftrightarrow f(x_1, \ldots, x_n) = 0$ oder $g(x_1, \ldots, x_n) = 0$. Z.b. ist $(X^2 - 1)$ nicht irreduzibel , da$(X^2 - 1) = (X + 1)(X - 1)$.

2.6 Faktorisierung von Polynomen

Voraussetzung :
R sei stets ein faktorieller Ring und K der Quotientenkörper Quot R von R.

Frage :
Gegeben sei ein Polynom $\tilde{f} \in K[X]$. Ist $\tilde{f} \in K[X]$ irreduzibel, wenn falls nicht wie sieht die Faktorisierung aus ?
Wir wissen, daß es a $\in K$ mit $f = a\tilde{f} \in R[X]$ ist primitiv für den Fall grad $f > 0$ und es gilt: $\tilde{f}$ irreduzibel in K[X] $\Leftrightarrow$ f irreduzibel in R[X].

Beispiel :
a) $\tilde{f} = \frac{3}{7}X^3 + \frac{1}{7}X + 5 \in \mathbb{Q}[X]$
b) $\tilde{g} = X^3 + \frac{1}{Y+1}X + 3 \in \mathbb{Q}(Y)[X]$
f=$3X^3 + X + 5$ ist irreduzibel, da der einzige möglich Ansatz für eine Zerlegeung $f = (aX^2 + bX + c)(eX + f)$ nach kurzer Rechnung keine Lösung für $a, b, c, e, f \in \mathbb{Z}$ hat. Somit ist $\tilde{f}$ ebenfalls irreduzibel.

Satz 1 :
Sei $f = \sum_{i=0}^{n} a_i X^i$ primitiv aus R[X] und $P \trianglelefteq R$ ein Primideal (mit $a_n \notin P$) und $\overline{f}$ definiert durch $\sum_{i=0}^{n} \overline{a}_i X^i \in R/P[X]$, wobei $\overline{a}_i = a_i + P$ sind.
a) So folgt aus der Irreduzibiltät von $\overline{f}$ in $R/P[X]$ diesselbige für f in R[X] (Beachte die Umkehrung ist im Allg. falsch!).
b) Und $f \in R[X]$ irreduzibel $\Leftrightarrow f(aX + b) \in R[X]$ irreduzibel, falls $a \in R^\star$ und $b \in R$

Beweis :
zu a): Die Abbildung $\varphi : R[X] \to R/P[X]$, $f \mapsto \overline{f}$ ist ein Homomorphismus, also folgt aus $f = g \cdot h \Rightarrow \overline{f} = \overline{g} \cdot \overline{h} \in R/P[X]$. Da wir annehmen $\overline{f}$ ist irreduzibel in $R/P[X]$, ist grad $\overline{g}$ oder grad $\overline{h}$ gleich 0. Wir betrachten den Leikoeffizient $a_n (\notin P$ nach Voraussetzung): $a_n = g_n \cdot h_n$, wobei g_n der Leikoeffizient von g und h_n der von h ist. Da $a_n \notin P \Rightarrow g_n \notin P \vee h_n \notin P$. Nun ist aber P gerade der Kern des Homomorphismus φ, d.h. nur Polynomen deren Leitkoeffizient aus P ist, werden auf Polynome geringeren Grades abgebildet, was aber hier nicht auftritt, da $g_n, h_n \notin P$.$\square$
zu b) Auch $\psi : R[X] \to R[X]$, $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i (aX + b)$ ist ein Homomorphismus sogar ein Isomorphismus, denn es existiert die Inverse $\psi^{-1} : R[X] \to R[X]$, $f \mapsto f(a^{-1}X - a^{-1}b)$. Also f irreduzibel $\Rightarrow \psi(f) = f(aX + b)$ irreduzibel.$\square$

Beispiel :
a) Seien $R = \mathbb{Z}, K = \mathbb{Q}$ und $f = 3X^3 + X + 35$. Wir wählen sinnvollerweise $P = 2\mathbb{Z}$, danit ist die Voraussetzung $a_n = 3 \notin P$ erfüllt. Dann ist $\varphi(f) = \varphi(3X^3 + X + 35) = X^3 + X + 1 \in \mathbb{F}_2[X]$ mit $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Wir nehmen an f sei reduzibel, dann ist nach Satz 1 $\overline{f} = \varphi(f) = X^3 + X + 1$ auch reduzibel, d.h. es gibt $\overline{g}, \overline{h} \in \mathbb{F}_2$ mit $\overline{f} = \overline{g} \cdot \overline{h}$. Auf Grund der Form von $\overline{f}$ können $\overline{g}$ und $\overline{h}$ nur die Form $\overline{f} = X^3 + X + 1 = (X^2 + bX + 1)(X + 1) = X^3 + (b + 1)X^2 + (b + 1) + X + 1$ haben. Aber egal ob $b = 0$ oder $b = 1 \in \mathbb{F}_2$ ist, erhalten wir einen Widerspruch. Folglich ist $\overline{f}$ in $R/P[X]$ und damit auch f in $R[X]$ irreduzibel.
b) Sei $g = (Y + 1)X^3 + X + 3(Y + 1) \in \mathbb{Z}[Y][X]$. Wähle $P = Y\mathbb{Z}[X]$, so ist $\overline{g} = X^3 + X + 3 \in \mathbb{Z}[Y][X]/P = \mathbb{Z}[X]$. Wir rechnen nur wie oben modulo 2 und erhalten aus $\overline{g}\, X^3 + X + 1$. Also ist auch g irreduzibel in $\mathbb{Z}[Y][X]$.

Eisensteinsche Irreduzibilitätskriterium :
Es sei $\sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv (ggt $a_i = 1$) und $p \in R$ ein Primelement mit $p \nmid a_n$, $p \mid a_i$ für $i < n$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.

Beweis :
Wir wählen $P = Rp$ und wenden auf f den Homomorphismus $\varphi : R[X] \to R/P[X]$, $f \mapsto \overline{f}$ an. So ist $\varphi(f) = \overline{f} = \sum_{i=0}^{n} \overline{a}_i X^i = \overline{a}_n X^n$. Wir nehmen an, f sei nicht irreduzibel, d.h. es existieren $g = \sum_{i=0}^{k} b_i X^i$ und $h = \sum_{i=0}^{l} c_i X^i$ für m = k+l. Da $p \mid a_0 = b_0 \cdot c_0$ und $p^2 \nmid a_0 = b_0 \cdot c_0$, gilt o.B.d.A. $p \mid c_0$ und $p \nmid b_0$. Setze nun $m = \max\{j | p \mid c_j\} < l$, denn $p \nmid a_n = b_k \cdot c_l$. Dann gilt $p \mid a_{m+1} = b_0 c_{m+1} + \underbrace{b_1 c_m + \ldots + b_{m+1} c_0}_{p|}$, d.h. aber $p \mid b_0 c_{m+1}$. Wegen der Wahl des m gilt, aber $p \nmid c_{m+1}$ und $p \nmid b_0$ nach obiger Überlegung. Was ein Widerspruch ist, d.h. f ist irreduzibel .$\square$

Beispiel :
Sei $f = 7X^{1000} + 25X^{73} + 15X + 5 \in \mathbb{Q}[X]$. Mit dem Eisensteinschen Kriterium für p=5, erhalten wir sofort, daß f irreduzibel

ist, da $p = 5 \nmid 7$, $5 \mid 25, 15$ und $p^2 = 25 \nmid 5$.

28. Vorlesung vom 8.1.2001

Beispiel :
a) Sei $f = X^n - pa \in \mathbb{Z}[X]$ mit $n \in \mathbb{N}$ und p Primzahl mit $p \nmid a$, dann ist f irreduzibel in $\mathbb{Z}[X]$ und somit auch in $\mathbb{Q}[X] =$ Quot $\mathbb{Z}$. Also gibt es in $\mathbb{Z}[X]$ oder auch in $\mathbb{Q}[X]$ irreduzible Polynome vom Grad ≥ 1
b) Sei $g = X^2 + Y^2 - 1 \in \mathbb{C}[X][Y]$. So ist $g = Y^2 + (X-1)(X+1)$ aufgefaßt als Polynom in Y. Wird können nun das Eisensteinsche Kriterium für die Primzahl $p = X - 1 \in \mathbb{C}[X]$ anwenden und damit ist g irreduzibel
c) Sei $h = X^2 + Y^2 + 1 \in \mathbb{C}[X][Y]$. Es folgt $h = Y^2 + (X+i)(X-i) \in \mathbb{C}[X][Y]$ ist wieder irreduzibel in $\mathbb{C}[X][Y]$ und damit auch in $R[X, Y]$

Satz 3 :
Ist p eine Primzahl, so ist $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$ in $\mathbb{Q}[X]$ irreduzibel.

Bemerkung :
Φ_p heißt Kreisteilungspolynom und $\Phi_p = \frac{X^p - 1}{X - 1} = \Pi_{i=1}^{p-1}(X - \xi_p^i)$ mit $\xi_p = e^{\frac{2\pi i}{p}}$.

Beweis :
Die Abbildung $\Psi : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \mapsto f(X+1)$ ist ein Ringisomorphismus. Dann ist $f \in \mathbb{Z}[X]$ irreduzibel $\Leftrightarrow f(X+1)$ irreduzibel in $\mathbb{Z}[X]$ ist. Wegen $X^p - 1 = (X-1) \cdot \phi_p \Rightarrow \Psi(X^p - 1) = \Psi(X-1) \cdot \Psi(\Phi_p) \Leftrightarrow (X+1)^p - 1 = \sum_{i=0}^{p} \binom{p}{i} X^i = X\Phi_p \Rightarrow \Phi_p = \sum_{i=0}^{p-1} \binom{p}{i} X^i$. Nun teilt p $\binom{p}{i}$ für $i = 1, \ldots, p-1$ und $p^2 \nmid a_0 = \binom{p}{p-1} = p$, was nach Eisenstein bedeutet, daß Φ_p irreduzibel ist .$\square$

Kapitel 3

Körper

3.1 Primkörper und Körpererweiterungen

R Sei ein Integritätsring, z.B. ein Körper. Wir definieren für $z \in \mathbb{Z}$ und $a \in R$: $z \cdot a := \begin{cases} \underbrace{a + \ldots + a}_{z} \text{ , } z \in \mathbb{N} \\ 0 \text{ , } z = 0 \\ -(\underbrace{a + \ldots + a}_{-z}) \text{ , } -z \in \mathbb{N} \end{cases}$

Dann ist $\psi : \mathbb{Z} \to R$, $n \mapsto n \cdot 1$ ein Ringhomomorphismus mit Kern $\Psi \trianglelefteq \mathbb{Z}$, da aber Ideale im Hauptidealring $\mathbb{Z}$ die Form $p\mathbb{Z}$ haben ist (Bild $\Psi \leq R$) Bild $\Psi \cong \mathbb{Z}/p\mathbb{Z}$ für eine Zahl $p \in Z$. Außerdem ist Bild Ψ ein Integritätsbereich, da Bild $\Psi \subseteq R$, also ist $p\mathbb{Z}$ ein Primideal, d.h. p ist eine Primzahl oder $p = 0$.

Definition :
Das so bestimmte $p \in \mathbb{Z}_{\geq 0}$ heißt **Charakteristik** von R oder kurz Char R. Es gilt Char R $= 0 \Leftrightarrow n \cdot 1 = \underbrace{1 + \ldots + 1}_{n} = 0 \Rightarrow$ $n = 0 \Leftrightarrow \Psi$ ist injektiv, bzw. Char R = p $> 0 \Leftrightarrow p \cdot 1 = \underbrace{1 + \ldots + 1}_{p} = 0$ und $p = min\{n \in \mathbb{N} | n \cdot 1 = 0\}$. Die Charakteristik eines Ringes ist also stets 0 oder eine Primzahl.

Definition :
Sei $(L, +, \cdot)$ Körper, dann heißt $K \subseteq L$ **Unterkörper**, wenn $(K, +|_{K \times K}, \cdot|_{K \times K})$ ein Körper ist. L heißt in diesem Fall **Oberkörper** von K oder **Erweiterungskörper**. Man kann L als K-Vektorraum betrachten, dann heißt $[L : K] := dim_K L$ **Körpergrad** bzw. auch Grad der Körpererweiterung.

Beispiel :
a) $\mathbb{Q} \subseteq \mathbb{R}$ mit $[\mathbb{R} : \mathbb{Q}] = \infty$
b) $\mathbb{R} \subseteq \mathbb{C}$ mit $[\mathbb{C} : \mathbb{R}] = 2$

Bemerkung :
Seien K_1, K_2 Unterkörper von L $\Rightarrow K_1 \cap K_2$ ist auch Unterkörper von L. Denn 1 = "Eins von L" $\in K_1, K_2$, demnach auch in $K_1 \cap K_2 \neq \emptyset$.

29. Vorlesung vom 10.1.2001

Satz 1 :
Ist K Körper, so ist der Primkörper von K $P(K) := \bigcap\{U | U$ Unterkörper von K $\}$ auch ein Körper. Ist weiter Char K $= 0$, so ist $P(K) \cong \mathbb{Q}$, und Char K $= p < \infty \Leftrightarrow P(K) \cong \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis :
Wir betrachten wieder den Ringhomomorphismus (siehe zuvor) $\Psi : \mathbb{Z} \to K, n \mapsto n \cdot 1_K$. Wegen $1 \in P(K) \Rightarrow m \cdot 1_K \in P(K)$ gilt $\Psi(\mathbb{Z}) \subseteq P(K)$. Ist nun Char K $= p$ Primzahl, so ist $\Psi(\mathbb{Z}) \cong \mathbb{F}_p$ Körper, demnach ist also $\mathbb{F}_p \cong P(K)$. Wenn Char K $= 0$, dann $\Psi(\mathbb{Z}) \cong \mathbb{Z}$. Der kleinste Körper der $\mathbb{Z}$ umfaßt und in K liegt ist somit $\mathbb{Q} =$ Quot $\mathbb{Z} = \{\frac{m}{n} | m \in \mathbb{Z}, n \in \mathbb{N}\} = P(K)$.□

Bemerkung :
D.h. umgekehrt, da in jedem Körper (bis auf Isomorphie) der Körper $\mathbb{Q}$ (für Char K=0) bzw. der Körper $\mathbb{F}_p$ (für Char K = p) enthalten ist, brauchen nur noch Körpererweiterungen von $\mathbb{Q}$ bzw. $\mathbb{F}_p$ zu betrachten, damit betrachten wir gleich alle möglichen Körper. Außerdem enthält jeder Körper K einen eindeutig bestimmten kleinsten Körper, nämlich den Primkörper $P(K)$ und es ist Char K = Char $P(K)$. Ist K endlich $\Rightarrow$ char K $= p > 0$

Beispiel :
Die Umkehrung gilt leider nicht, da $\mathbb{F}_p(X) = \text{Quot}\,(\mathbb{F}_p[X])$ ist ein unendlicher Körper mit Char K $= p$. Ist aber K endlich, dann $[K : \mathbb{F}_p] = dim_{\mathbb{F}_p} K = n < \infty$ und $K \cong \mathbb{F}_p^n$ als $\mathbb{F}_p$-Vektorraum, d.h. $|K| = p^n$. Also gibt es keinen Körper K mit $|K| \in \{6, 10, 12\}$, weil 6, 10 und 12 keine Primzahlpotenzen sind.

Gradsatz :
Seien $K \subseteq L \subseteq M$ Körpererweiterungen. So ist $[M : K] = [M : L] \cdot [L : K]$.

Beweis :
Sei $B_1 = (x_\alpha)_{\alpha \in A}$ eine K-Basis von L, wobei man L als K-Vektorraum auffaßt und $B_2 = (y_\beta)_{\beta \in B}$ eine L-Basis von M. Dann ist $|A| = [L : K]$ und $|B| = [M : L]$. Wir behaupten, daß $B_3 := (x_\alpha y_\beta)_{(\alpha,\beta) \in A \times B}$ eine K-Basis von M ist, dann ist $[M : K] = |A \times B| = |A| \cdot |B| = [M : L] \cdot [L : K]$.
zu B_3 ist ein Erzeugendensystem: Sei $z \in M$ beliebig, so existieren nach Voraussetzung ein $z_\beta \in L$ mit $z_\beta = \sum_{\beta \in B_2} z_\beta \cdot y_\beta$ mit $z_\beta \neq 0$ nur für endlich viele. Zu jedem β existieren aber auch $a_{\alpha\beta} \in K$ mit $z_\beta = \sum_{\alpha \in A} a_{\alpha\beta} x_\alpha$. Einsetzt ergibt sich $z = \sum_{\beta \in B} \sum_{\alpha \in A} \underbrace{a_{\alpha\beta}}_{\in K} \underbrace{x_\alpha y_\beta}_{\in B_3} \cdot \square$
zu B_3 ist K-linear unabhängig: Wir nehmen an, $0 = \sum_{\alpha \in A} \sum_{\beta \in B} a_{\alpha\beta} x_\alpha y_\beta$ und $a_{\alpha\beta} \neq 0$ für nur endlich viele. Dann $0 = \sum_{\beta \in B} \underbrace{\sum_{\alpha \in A} a_{\alpha\beta} x_\alpha}_{\in L} y_\beta$, da aber $B_2 = (y_\beta)_{\beta \in B}$ L-linear unabhängig ist, folgt $\sum_{\alpha \in A} a_{\alpha\beta} x_\alpha = 0$. Und da B_1 K-linear unabhängig ist, folgt $\forall \alpha \in A \forall \beta \in B : a_{\alpha\beta} = 0$.$\square$

Folgerung :
Ist $[M : K] = p$ ein Primzahl, so existieren keine Zwischenkörper L mit $K \subseteq L \subseteq M$, außer $L = K$ oder $L = M$.

Beispiel :
a) Sei $|K| = 8 = 2^3$, dann ist $|K : \mathbb{F}_2| = 3$. Die einzigen Unterkörper von K sind, also $P(K) = \mathbb{F}_2$ und K.
Man kann nach Lagrange sagen, daß U Unterkörper K $\Rightarrow (U, +) \leq (K, +) \Rightarrow |U| \mid |K| = 2^3$. Und $(U \setminus \{0\}, \cdot) \leq (K \setminus \{0\}, \cdot) \Rightarrow |U| - 1 \mid |K| - 1$
b) Sei K Körper mit $|K| = 3^4$, so $[K : \mathbb{F}_3] = 4$. Nach Lagrange gilt für einen weiter Unterkörper U von K: $|U| \in \{3, 9, 27, 81\}$ und $|U| - 1 \mid 80$, insgesamt bleibt nur $|U| \in \{3, 9, 81\}$, da $26 \nmid 80$.

3.2 Algebraische und transzendente Elemente

Definition :
Sei $L \supseteq K$ ein Körpererweiterung. $\alpha \in L$ heißt **algebraisch** über K, wenn es $\exists 0 \neq f \in K[X]$ mit $f(\alpha) = 0$ und sonst **transzendent** über K.

Beispiele :
a) $\sqrt[3]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn $\exists f = X^3 - 2 \in \mathbb{Q}[X]$ mit $f(\alpha) = 0$.
b) Sei K ein beliebiger Körper, betrachte $L = K(X) = \text{Quot}(K[X]) \supseteq K$, so ist X transzendent über K.
c) $e = \sum \frac{!}{i!} \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (gezeigt von Hermit 1873) sowie π (nach Lindemann 1882).

Lemma 1 :
Ist $L \supseteq K$ Körpererweiterung und $\alpha \in L$ algebraisch über K, dann gibt es genau ein Polynom $f_\alpha \in K[X]$ mit
a) $g \in K[X] \wedge g(\alpha) = 0 \Rightarrow f_\alpha \mid g$
b) f_α ist normiert, d.h. $f_\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ $(a_n = 1)$
Und $f_\alpha \in K[X]$ ist einziges irreduzibles normiertes Polynom in $K[X]$ mit Nullstelle α.

Definition :
Wir nennen das Polynom f_α, welches in Lemma 1 charakterisiert wurde, das **Minimalpolynom** von α über K.

Beweis :
Es gilt $I = \{g \in K[X] | g(\alpha) = \text{o}\} \trianglelefteq K[X]$, denn sei $g \in I$ und $k \in K[X] \Rightarrow k \cdot g$ hat die Nullstelle α also liegt in I, wegen $(k \cdot g)(\alpha) = k(\alpha) \cdot g(\alpha)$. $I \neq \emptyset$, weil α algebraisch über K ist. $\exists f \in K[X] : I = (f) = K[X] \cdot f$ und $(f) = (cf)$ für $c \in K^\star = K \setminus \{0\}$. Aber in $\{f \in K[X] | (f) = I\}$ existiert genau ein normiertes Polynom. Sei nun $\Psi_\alpha : K[X] \to L$, $g \mapsto g(\alpha)$ der Einsetzungshomomorphismus, so ist der Kern Ψ gerade $I = (f_\alpha)$. Nach dem Homomorphiesatz ist $L \geq \text{Bild}\ \Psi \cong K[X]/(f_\alpha)$. Da L ein Körper, also insbesondere ein Integritätsring ist, ist Bild Ψ auch einer und damit ist (f_α) ein Primideal. D.h. f_α ist irreduzibel über $K[X]$.$\square$

30. Vorlesung vom 12.1.2001

Vergleichen Sie die beiden folgenden Ringhomomorphismen:
a) Ψ sei der bekannte Ringhomomorphismus $\Psi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$, so $\exists p \in \mathbb{Z} : (p) = \text{Kern } \Psi \trianglelefteq \mathbb{Z}$ Hauptidealring.
1. Fall $p = 0$: so ist Ψ injektiv, d.h. $\mathbb{Z} \cong \Psi(\mathbb{Z})$ und Char K = 0.
2. Fall $p > 0$: $K \geq \Psi(\mathbb{Z}) \cong \mathbb{Z}/(p)$, falls p eine Primzahl ist und $\Psi(\mathbb{Z})$ ist Integritätsring
b) Sei Ψ_α der Einsetzungshomomorphismus $\Psi_\alpha : K[X] \to K$, $\sum b_i X^i \mapsto \sum b_i \alpha^i$. So $\exists f \in K[X]$ mit $(f) = \text{Kern } \Psi_\alpha \trianglelefteq K[X]$ Hauptidealring.
1. Fall $f = 0$: so ist Ψ_α injektiv und α ist transzendent über K.
2. Fall $f \neq 0$: so $\exists$ normiertes $f_\alpha \in K[X](f) = (f_\alpha)$ und $L \geq \Psi_\alpha(K[X]) \cong K[X]/(f_\alpha)$, wobei $\Psi_\alpha(K[X])$ ein Integritätsring ist und da f_α irreduzibel (hier gleich Primelement) ist, folgt $\Psi_\alpha(K[X])$ ist ein Körper.
Die folgenden 6 Aussagen sind für einen Hauptidealring R und $a \in R$ mit $\{0\} \neq (a) \trianglelefteq R$ äquivalent:
$R/(a)$ ist Integritätsring $\Leftrightarrow$
(a) ist Primideal $\Leftrightarrow$
a ist Primelement $\Leftrightarrow$
a ist irreduzibel $\Leftrightarrow$
(a) ist maximales Ideal $\Leftrightarrow$
$R/(a)$ ist ein Körper

Bezeichnung :
$K[\alpha] = \{\sum_{i=0}^{n} b_i \alpha^i | n \in \mathbb{N}_0, b_i \in K\} = \Psi_\alpha(K[X])$ ist der kleinste Teilring in L, der K und α enthält.

Satz 1 :
Sei $L \supseteq K$ ein Körpererweiterung und $\alpha \in$ L.
a) Ist α transzendent über K, so ist $K[\alpha] \cong K[X]$.
b) Falls α algebraisch über K ist mit Minimalpolynom $f_\alpha \in K[X]$, so ist $K[\alpha] \cong K[X]/(f_\alpha)$ ein Körper mit $[K[\alpha] : K] =$ Grad $f_\alpha = n$ und $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine K-Basis von $K[\alpha]$.

Beweis :

Schlüsselwörter

Automorphismus, 17
äquivariant, 8

Bahn, 6

direktes Produkt, 19

Eulersche Φ-Funktion, 18

Gruppe, 3
    einfach, 23
    erzeugte, 4
    Homomorphismus, 5
    nilpotent, 22
    p-Gruppe, 10
Sylowgruppe, 21
    zyklisch, 4

Halbgruppe, 3

Index, 8

Kern, 14
Komplexprodukt, 13
Konjugation, 5
Konjuguiertenklassen, 9

Monoid, 3
Morphismus, 8

Nebenklasse, 8
Normalisator, 11
Normalteiler, 13

Ordnung, 4
Operation, 4
    treu, 6
    transitiv, 7
Ω-Operatorgruppe, 15
    Ω-Homomorphismus, 15

Reihe, 23
    äquivalent, 23
    Haupt-, 23
    Kompositions-, 23
    Normal-, 23
    Subnormal-, 23

Stabilisator, 7
Sylowgruppe, 21

Transversale, 12

Untergruppe, 4
    charakteristisch, 17
    konjugiert, 7
    Ω-invariant, 15
    Ω-zulässig, 15

Verband, 16
    Verbandisomorphismus, 16

Zentralisator, 9
Zentrum, 10

Literaturverzeichnis

nach Autoren:
Meyberg I bzw. II
Hornfeck
Bosch
Herstein
F.Lorenz
Stroth
Jacobson Basic Algebra I bzw. II