Tutorium #5: 5.12.2014

Auflösbarkeit von Gruppen, etwas Ring-Theorie und evtl. Körper-Erweiterungen

⓪ Motivation

Gleichung	gibt es „Formel" für x?	Grund	
$x^2+px+q=0$	ja, $x_{1,2}=-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}$	Σ_2	auflösbare Gruppen
$x^3+px^2+qx+r=0$	ja	Σ_3	
$x^4+\dots=0$	ja	Σ_4	
$x^5+px^4+qx^3+rx^2+sx+t=0$	nein	Σ_5 nicht auflösbar	
$p,q,r,s,t\in\mathbb{C}$		Begründung: Galois-Theorie.	

① Auflösbarkeit - Def. und Bsp.

G Gruppe [nicht unbedingt endlich]

Def.: G ist auflösbar $\Leftrightarrow$ es gibt Untergruppen $G_1,\dots,G_{n-1}$ in G so dass

$$G=G_0\rhd G_1\rhd\dots\rhd G_i\rhd G_{i+1}\rhd\dots\rhd G_{n-1}\rhd G_n=\{e\}$$

und G_i/G_{i+1} abelsch $\forall i\in\{0,\dots,n-1\}$.

Beispiele:

1) G abelsch, insb. $\mathbb{Z}_m$, V_4. [$G=G_0\rhd G_1=\{e\}$]

2) D_m, Σ_4, A_4, insb. $\Sigma_3\cong D_3$, $\Sigma_2\cong\mathbb{Z}_2$ $m\in\mathbb{N}$ [siehe VL]

3) p-Gruppen, [insb. p-Sylow-UG]

Bem.: A_5 einfach & nicht abelsch $\Rightarrow$ nicht auflösbar

G mit $|G|<59\Rightarrow G$ auflösbar.

[A_5 ist die kleinste nicht auflösbare Gruppe]

② Kommutatoren-Reihe

G Gruppe $\rightsquigarrow G' := [G,G] = \langle xyx^{-1}y^{-1} \mid x,y \in G \rangle$
Kommutator

es gilt:
- $[G,G] \triangleleft G$, [denn $g(xyx^{-1}y^{-1})g^{-1} \in [G,G]$]
- $G/_{[G,G]}$ abelsch $=: G^{ab}$ [denn $xy[G,G] = yx[G,G]$]
- $K \triangleleft G$, $G/_K$ abelsch $\Rightarrow [G,G] \subset K$

[Kommutator = kleinster Normalteiler K so dass $G/_K$ abelsch]

$G^{(1)} = G' \quad G^{(i+1)} := [G^{(i)}, G^{(i)}]$

$\Rightarrow G \rhd G^{(1)} \rhd G^{(2)} \rhd \dots \rhd G^{(i)} \rhd G^{(i+1)} \rhd \dots$ [Kommutatoren-Reihe / Filtration]
mit $G^{(i)}/_{G^{(i+1)}}$ abelsch

entweder $\exists n \in \mathbb{N}: G^{(n)} = \{e\} \Rightarrow G$ auflösbar

↳ oder $\exists n \in \mathbb{N}: G^{(n)} = G^{(n+1)} \neq \{e\} \Rightarrow G$ nicht auflösbar

③ Kriterien für Auflösbarkeit

(1) $H \subset G$ uG, G auflösbar $\Rightarrow H$ auflösbar

(2) $K \triangleleft G$ G auflösbar $\Leftrightarrow K$ und $G/_K$ auflösbar

(3) $\exists n \in \mathbb{N}: G^{(n)} = \{e\}$ $\Leftrightarrow G$ auflösbar
[gilt auch falls $|G| < \infty$.]

Korollar 1: Sei $n \geq 5$, $A_5 \subset \Sigma_n$ (nicht auflösbar) $\overset{A1)}{\Rightarrow} \Sigma_n$ nicht auflösbar $\forall n \geq 5$
[Gleichungen n.-ten Grades nicht durch Formel]

Korollar 2: Sei G_1 abelsch und G_2 auflösbar [z.B. auch abelsch]

$\Rightarrow G = G_1 \times G_2 \rhd G_2 = K$ } auflösbar $\overset{A2)}{\Rightarrow} G_1 \times G_2$ auflösbar
$G/_K \cong G_1$

z.B. $\mathbb{Z}_m \times \mathbb{Z}_n$.

④ $G = T_3(K) = \left\{ \begin{pmatrix} a & d & f \\ 0 & b & e \\ 0 & 0 & c \end{pmatrix} \in GL_3(K) \right\}$

Beh.: G ist auflösbar

[falls $|K| = \infty \Rightarrow |G| = \infty$]

Ansatz: bilde $G', G'', \ldots$

$G' = \langle \underbrace{xyx^{-1}y^{-1}}_{} \mid x, y \in G \rangle$

$$\begin{pmatrix} a_1 & * & * \\ 0 & b_1 & * \\ 0 & 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & * & * \\ 0 & b_2 & * \\ 0 & 0 & c_2 \end{pmatrix}\begin{pmatrix} a_1^{-1} & x & x \\ & b_1^{-1} & x \\ & & c_1^{-1} \end{pmatrix}\begin{pmatrix} a_2^{-1} & x & x \\ & b_2^{-1} & x \\ & & c_2^{-1} \end{pmatrix}$$
$$x \qquad\qquad y \qquad\qquad x^{-1} \qquad\qquad$$

$$= \begin{pmatrix} a_1a_2 & x & x \\ & b_1b_2 & x \\ & & c_1c_2 \end{pmatrix}\begin{pmatrix} a_1^{-1}a_2^{-1} & x & x \\ & b_1^{-1}b_2^{-1} & x \\ & & c_1^{-1}c_2^{-1} \end{pmatrix} = \begin{pmatrix} 1 & x & x \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow G' \in F = \left\{ \begin{pmatrix} 1 & d & f \\ & 1 & e \\ & & 1 \end{pmatrix} \mid d, e, f \in K \right\}$$

Hoffnung: $F' = \{e\}$, denn $G'' = [G', G'] \subset [F, F] = F'$

[$H \subset G \Rightarrow [H, H] \subset [G, G]$]

$$\Rightarrow xyx^{-1}y^{-1} = \begin{pmatrix} 1 & d_1 & x \\ & 1 & e_1 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & d_2 & x \\ & 1 & e_2 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & -d_1 & x \\ & 1 & -e_1 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & -d_2 & x \\ & 1 & -e_2 \\ & & 1 \end{pmatrix}$$
$$x \qquad\qquad y \qquad\qquad x^{-1} \qquad\qquad y^{-1}$$

$$= \begin{pmatrix} 1 & d_1+d_2 & * \\ & 1 & e_1+e_2 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & -d_1-d_2 & x \\ & 1 & -e_1-e_2 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

$$\Rightarrow F' \subset E = \left\{ \begin{pmatrix} 1 & 0 & f \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid f \in K \right\}$$

E ist abelsch: $\begin{pmatrix} 1 & & f_1 \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & f_2 \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & f_2+f_1 \\ & 1 & 0 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & f_2 \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & f_1 \\ & 1 & \\ & & 1 \end{pmatrix}$

$\Rightarrow E' = \{e\}$

$$\begin{array}{ccccc} G & \rhd & G' & \rhd & G'' \rhd G''' \\ \cup & & \cup & & \cup \\ F & \rhd & F' & \rhd & F'' \Rightarrow G''' = \{e\} \Rightarrow G \text{ auflösbar} \\ \cup & & \cup & & \cup \\ E & \rhd & E' = \{e\} & & \end{array}$$

Zusammenfassung: [Abschätzen von Kommutatoren]

③

⑤ Unterringe und Ideale

R Ring, $M \subset R$

- M Unterring $\Leftrightarrow$ a) $\forall x,y \in M$: $\left.\begin{array}{l} x+y \in M \\ -x \in M \\ 0_R \in M \end{array}\right\}$ $(M,+) \subset (R,+)$ UG.

b) $\forall x,y \in M$: $x \cdot y \in M$ c) $1_R \in M$

Bsp.: $\mathbb{Z} \subset \mathbb{Q}$.

M Ideal $\Leftrightarrow$ a) $(M,+) \subset (R,+)$ UG

B) $\forall r \in R \; \forall x \in M$: $r \cdot x \in M$.

Bem.: [M Ideal mit $1_R \Rightarrow M = R$] [Bem.: B) $\Rightarrow$ B).]

Bsp.: $m\mathbb{Z} \subset \mathbb{Z}$

Sei $R = \{ f : [0,1] \cup \longrightarrow \mathbb{R} \}$ $\rightsquigarrow$ R ein Ring [kommutativ]

$[0, \frac{1}{2}] =: A$

$(f+g)(z) = f(z) + g(z)$ $\quad 0_R : z \longmapsto 0$

$(f \cdot g)(z) = f(z) \cdot g(z)$ $\quad 1_R : z \longmapsto 1$

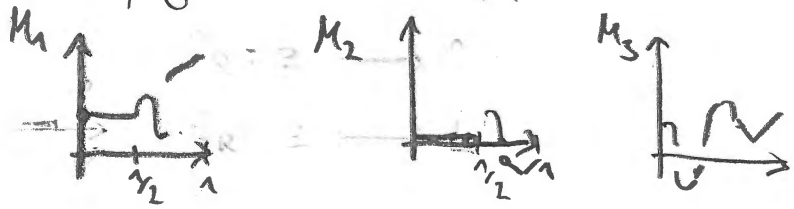
Seien

$M_1 = \{ f \in R \mid f$ konstant auf $A \}$

$M_2 = \{ f \in R \mid f(a) = 0 \; \forall a \in A \}$

$M_3 = \{ f \in R \mid f(a) \neq 0 \; \forall a \in A \}$

$M_4 = \{ f \in R \mid f(a) = 0$ für alle bis auf endlich viele $a \in A \}$



Was davon sind Unterringe oder Ideale?

$f,g \in M_i$	$f+g \in M_i$	$-f \in M_i$	$0 \in M$	$f \cdot g \in M_i$	$1_R \in M_i$	$r \cdot f \in M$ ($r \in R$)	
M_1	✓	✓	✓	✓	✓	$x \cdot f \notin M_1$	Unterring
M_2	✓	✓	✓	✓	✓	✓	Ideal
M_3	$f+(-f) \notin M_3$	✓	✓	✓	✓	$0 \cdot f \notin M_3$	–
M_4	✓	✓	✓	✓	✓	✓	Ideal

a) B) & c) B)

⑥ Bem. zu Homomorphismen

1) was ist $\mathrm{Hom}_{\mathrm{Gr}}(\mathbb{Z}, \mathbb{Q})$?

$$= \{\varphi : (\mathbb{Z},+) \longrightarrow (\mathbb{Q},+) \mid \varphi(0)=0,\ \varphi(k+\ell)=\varphi(k)+\varphi(\ell)\}$$

$$\Rightarrow \varphi(-k) = -\varphi(k)$$

sei $a \in \mathbb{Q}$ mit $\varphi(1)=a$ $\Rightarrow$

$$\Rightarrow \varphi(n) = \varphi(\underbrace{1+\ldots+1}_{n}) = \underbrace{a+\ldots+a}_{n\text{-mal}} = n\cdot a \qquad n \in \mathbb{N}^+$$

und $\varphi(-n) = -\varphi(n)$ $\Rightarrow$ φ eindeutig durch $\varphi(1) \in \mathbb{Q}$ festgelegt

$$\Rightarrow \mathrm{Hom}_{\mathrm{Gr}}(\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}$$

$$\varphi \longmapsto \varphi(1)$$

$$(\varphi_a : 1 \longmapsto a) \longleftarrow\!\shortmid\ a$$

2) was ist $\mathrm{Hom}_{\mathrm{rings}}(\mathbb{Z}, \mathbb{Q})$?

$$= \{\psi : (\mathbb{Z},+,\cdot) \longrightarrow (\mathbb{Q},+,\cdot) \mid \psi(0)=0,\ \psi(k+\ell)=\psi(k)+\psi(\ell),\ \psi(1)=1,\ \psi(k\cdot\ell)=\psi(k)\cdot\psi(\ell)\}$$

- $\psi(1)=1 \Rightarrow \psi(k)=k$ $\Rightarrow$ $\mathrm{Hom}_{\mathrm{rings}}(\mathbb{Z}, \mathbb{Q}) = \{\psi\}$

  „$a=1$"

$\psi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ kanonische Einbettung

$z \longmapsto z$

Bem.:

a) $\mathrm{Hom}_{\mathrm{Gr}}(G,H) \ni \varphi : G \longrightarrow H$, $g \longmapsto e$

$H \neq \emptyset$

b) $\mathrm{Hom}_{\mathrm{rings}}(R,S)$ kann leer sein:

z.B. $R=\mathbb{Z}_3$ $S=\mathbb{Z}$

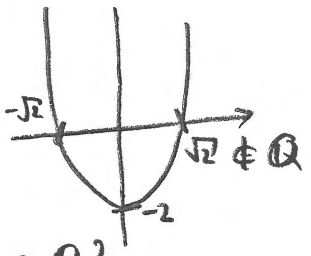
Ang.: $\exists \varphi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}$, $\bar{0} \longmapsto 0$, $\bar{1} \longmapsto 1$ Ring Hom. $\Rightarrow \varphi(\bar{1}) = 1$

$\Rightarrow 0 = \varphi(\bar{0}) = \varphi(\bar{4}) = \varphi(\bar{1}+\bar{1}+\bar{1}+\bar{1})$ $\Rightarrow \mathrm{Hom}_{\mathrm{rings}}(\mathbb{Z}_4, \mathbb{Z}) = \emptyset$

⑦ Körper-Erweiterungen

betrachte $x^2 - 2 = 0$ (*)

keine Lsg. $x \in \mathbb{Q}$



definiere $\mathbb{Q}[\sqrt{2}] := \{a + \sqrt{2}\,b \mid a, b \in \mathbb{Q}\}$

(*) hat 2 Lösungen $x \in \mathbb{Q}[\sqrt{2}]$.

Bem.: $\mathbb{Q}[\sqrt{2}]$ ist ein Ring. [Unterring von $\mathbb{R}$]

z.B. $(a+\sqrt{2}\,b)\cdot(c+\sqrt{2}\,d) = (ac + 2bd) + \sqrt{2}\,(bc + ad) \in \mathbb{Q}[\sqrt{2}]$

ist $\mathbb{Q}[\sqrt{2}]$ ein Körper? $\rightsquigarrow$ was wäre $(a+\sqrt{2}\,b)^{-1}$ $(a \neq 0 \neq b)$.

betrachte $\mathbb{C} = \{\underbrace{a + ib}_{z} \mid a, b \in \mathbb{R}\} =$ „$\mathbb{R}[i]$" $\leftsquigarrow$ $x^2 + 1 = 0$ mit $x \in \mathbb{R}$

$z \cdot \bar{z} = |z|^2 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2}$ $\forall z \neq 0$.

analog für $\mathbb{Q}[\sqrt{2}]$:

$(a+\sqrt{2}\,b)(a-\sqrt{2}\,b) = a^2 - 2b^2$ $\quad | : (a^2 - 2b^2)$

- $a^2 - 2b^2 = 0 \iff a = \pm\sqrt{2}\,b$
- $a, b \in \mathbb{Q}$, $a \neq 0 \neq b \Rightarrow a^2 - 2b^2 \neq 0$

$(a+\sqrt{2}\,b)\,\frac{a-\sqrt{2}\,b}{a^2-2b^2} = 1 \Rightarrow (a+\sqrt{2}\,b)^{-1} = \underbrace{\frac{a}{a^2-2b^2}}_{\in \mathbb{Q}} - \sqrt{2}\,\underbrace{\frac{b}{a^2-2b^2}}_{\in \mathbb{Q}}$.

$\Rightarrow \mathbb{Q}[\sqrt{2}]$ ein Körper. „Erweiterung von $\mathbb{Q}$".

Ist $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + \sqrt{2}\,b + \sqrt{3}\,c + \sqrt{6}\,d \mid a, b, c, d \in \mathbb{Q}\}$ ein Körper?

ja. $\rightsquigarrow$ VL.

Bem. zu „G auflösbar $\Rightarrow G^{(n)} = \{e\}$ $\exists n \in \mathbb{N}$"

$G = G_0 \rhd G_1 \rhd \dots \rhd G_n = \{e\}$

G_1/G_0 abelsch $\Rightarrow G_1 \supset [G, G] \Rightarrow \dots \Rightarrow G_n \supset G^{(n)}$. (Induktion)

$\| \; \{e\}$

[$G_i \supset G^{(i)}$ $\quad G_i \rhd G_{i+1}$, G_i/G_{i+1} abelsch $\Rightarrow G_{i+1} \supset [G_i, G_i] \supset [G^{(i)}, G^{(i)}] = G^{(i+1)}$]

Zusammenfassung:

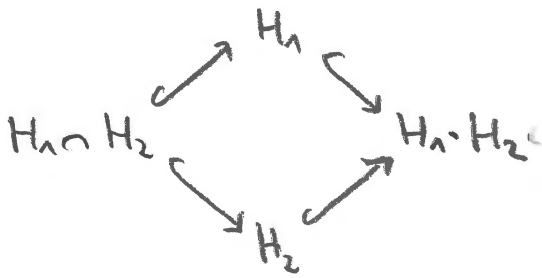
$$\begin{array}{ccccc} & & E & \triangleright & E' = \{e\} \\ & & \cup & & \cup \\ & F & \triangleright & F' & \triangleright & F'' \\ & \cup & & \cup & & \cup \\ G & \triangleright & G' & \triangleright & G'' & \triangleright & G''' \end{array} \quad \Rightarrow G''' = \{e\} \Rightarrow G \text{ auflösbar.}$$

[„Abschätzungen" von Kommutatoren]

Lemma: Sei $H_1 \triangleleft G$, $H_2 \triangleleft G$ mit H_1, H_2 auflösbar

$\Rightarrow H_1 \cdot H_2 \triangleleft G$ mit $H_1 \cdot H_2$ auflösbar
a) b)

Bew.:



$H_1 \triangleleft G, H_2 \triangleleft G$ H_1

$\Rightarrow g H_1 \cdot H_2 = H_1 g H_2 = H_1 H_2 g \quad \forall g \in G$

$\Rightarrow H_1 \cdot H_2 \triangleleft G$

a)

$H_1 \triangleleft G \Rightarrow H_1 \triangleleft H_1 \cdot H_2$ $\quad H_1 \cdot H_2 / H_1 \cong H_2 / H_1 \cap H_2$ und $H_1 \cap H_2 \triangleleft H_2$

H_2 auflösbar $\overset{A2)}{\Rightarrow}$ $H_2 / H_1 \cap H_2$ auflösbar

$\Rightarrow H_1 \cdot H_2$ auflösbar

Corollar: Jede endliche Gruppe hat eine eindeutige größte normale auflösbare UG.

Bew.: Seien $H_1, \dots, H_n$ alle normalen auflösbaren UG von G

$\rightsquigarrow H = H_1 \cdot \dots \cdot H_n$ ist die größte. [$|G|$ endlich $\Rightarrow$ endlich viele UG]

Tutorium #6: 12.12.2014

(Integritäts-) Ringe

① Nullteiler und Einheiten

R ein Ring [kommutativ, mit $1 \neq 0$]

Def.: Sei $a \in R$ mit $a \neq 0$.

- a ist <u>Nullteiler</u> $\Leftrightarrow \exists r \in R \setminus \{0\}: \; r \cdot a = 0$ „a teilt 0"
- a ist <u>Einheit</u> $\Leftrightarrow \exists r \in R: \; r \cdot a = 1$ „a teilt 1"

in diesem Fall: $r \neq 0$ und $r = a^{-1}$ „a invertierbar"

<u>Notation</u>: $R^* =$ Einheiten von R

$R^0 =$ Nullteiler

$R^c = R \setminus (R_0 \cup R^*)$

Bem.: $R^* \cap R^0 = \emptyset$

[Ang. $\exists a \in R^* \cap R^0 \Rightarrow \exists r_0, r_1 \in R \setminus \{0\}$: $r_0 \cdot a = 0$, $r_1 \cdot a = 1$

$\Rightarrow 0 = r_0 \cdot r_1 \cdot a = r_0$ ↯]

$\Rightarrow R = R^* \dot\cup R^0 \dot\cup R^c$ (mit $1 \in R^*$, $0 \in R^0$)

Bsp.:

R	R^*	R^0	R^c
$\mathbb{Z}$	$\{1, -1\}$	$\emptyset$	...
$K[x]$	K^*	$\emptyset$	...)
$\mathbb{Z}_6$	$\{\bar 1, \bar 5\}$	$\{\bar 2, \bar 3, \bar 4\}$	$\{\bar 0\}$
$K[x]/(x^n)$	K^*	(x)	$\{\bar 0\}$)

Bem.: R ein <u>Körper</u> $\Leftrightarrow R = R^* \cup \{0\}$ (

$\Leftrightarrow R^0 = \emptyset$ und $R^c = \{0\}$.

Def.: R <u>nullteilerfrei</u> / <u>Integritätsring</u> / <u>Integritätsbereich</u> „IR"

$\Leftrightarrow R^0 = \emptyset$.

$\Leftrightarrow \forall a, b \in R \setminus \{0\} : \; a \cdot b \neq 0$.

Bem.: $a, b \in R^* \Rightarrow b \cdot a \in R^*$ ↑ [nach oben]

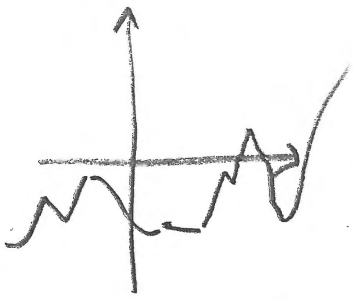
$a \in R^0, r \in R^0 \setminus \{0\} \Rightarrow r \cdot a \in R^0$

② Zwei Funktionenringe

$R_1 = C^0(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{R} \text{ stetig} \}$

$\vee$

$[R_2 = C^\infty(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{R} \text{ bel. oft diff'bar} \}]$

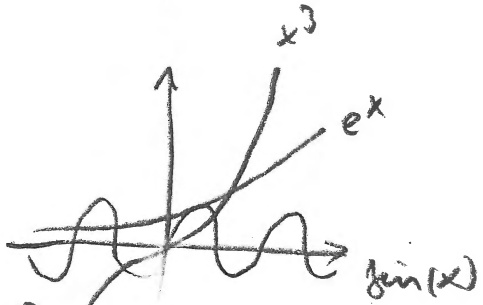


Frage:

a) Ist R_1 ein YR?

$[R_2]$ $[e^{-\frac{1}{x^2}}]$

· Nein, z.B. $f(x) = \begin{cases} x & x > 0 \\ 0 & x \leq 0 \end{cases}$ $g(x) = \begin{cases} 0 & x > 0 \\ -x & x \leq 0 \end{cases}$



$\Rightarrow f \cdot g = 0$ mit $f \neq 0, g \neq 0$.

b) R_1^*?

Seien $f, g \in R_1$ so dass $f \cdot g = 1 \Rightarrow f(x) \cdot g(x) = 1 \ \forall x \in \mathbb{R}$

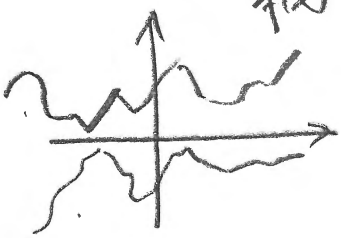
$\Rightarrow f(x) \neq 0 \Rightarrow g(x) = \frac{1}{f(x)}$

Beh.:

$= R_1^* = \{ f \in R_1 \mid f(x) \neq 0 \ \forall x \in \mathbb{R} \}$

$= \{ f \in R_1 \mid f(x) > 0 \ \forall x \in \mathbb{R} \}$

$\dot{\cup} \{ f \in R_1 \mid f(x) < 0 \ \forall x \in \mathbb{R} \}$



„$\subseteq$": ✓ bew.

„$\supseteq$": $f \in R_1$ mit $f(x) \neq 0 \Rightarrow f^{-1}(x) = \frac{1}{f(x)} \in C^0(\mathbb{R})$.

③ Endliche Ringe

R endlich $\rightsquigarrow$ R^* R^0 R^c

a) $\mathbb{Z}_p$ $\{\bar{1}, \dots, \overline{p-1}\}$ $\emptyset$ $\{\bar{0}\}$ Körper

b) $\mathbb{Z}_4$ $\{\bar{1}, \bar{3}\}$ $\{\bar{2}\}$ $\{\bar{0}\}$

$[\bar{3}^2 = \bar{9} = \bar{1}]$

$\mathbb{Z}_6$ $\{\bar{1}, \bar{5}\}$ $\{\bar{2}, \bar{3}, \bar{4}\}$ $\{\bar{0}\}$

$\bar{5} = \bar{25} = \bar{1}$ $\bar{2}\cdot\bar{3} = \bar{0} = \bar{4}\cdot\bar{3}$

$\mathbb{Z}_8$ $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ $\{\bar{2}, \bar{4}, \bar{6}\}$ $\{\bar{0}\}$

c)
$$K[X]/(X^n) = \{\sum_{i=0}^{n-1} a_i \bar{X}^i\} \qquad \bar{X}^i \cdot \bar{X}^{n-i} = \bar{X}^n = \bar{0}$$

$K[X]/(X^n)$ K^* $(\bar{X}) = \langle \bar{X}, \dots, \bar{X}^{n-1} \rangle_K$ $\{\bar{0}\}$.

d)
$$\mathbb{Z}_2[X]/(X^3) = \{\bar{0}, \bar{1}, \bar{X}, \bar{X}+\bar{1}, \bar{X}^2, \bar{X}^2+\bar{X}, \bar{X}^2+\bar{1}, \bar{X}^2+\bar{X}+\bar{1}\}$$

$\bar{X}$ $\in R^0$; $\bar{X}^2$ $\in R^0$; $\bar{X}^2+\bar{X} = \bar{X}(\bar{X}^2+\bar{1})$ $\in R^0$; $\bar{X}^2+\bar{1}$ $\in R^*$ wegen $(\bar{X}+\bar{1})^2$; $\bar{X}^2+\bar{X}+\bar{1}$ $\in R^*$

- $\bar{X}\cdot\bar{X}^2 = \bar{0}$
- $(\bar{X}+\bar{1})^2 = \bar{X}^2 + \bar{2}\bar{X} + \bar{1} = (\bar{X}^2+\bar{1})$
- $(\bar{X}+\bar{1})(\bar{X}+\bar{1}+\bar{X}^2) = (\bar{X}^2+\bar{1}) + \bar{X}^2(\bar{X}+\bar{1}) = \bar{2}\bar{X}^2 + \bar{1} = \bar{1}$

	R^*	R^0	R^c
	$\bar{1}$, $\bar{X}+\bar{1}$, $\bar{X}^2+\bar{1}$, $\bar{X}^2+\bar{X}+\bar{1}$	$\bar{X}$, $\bar{X}^2$, $\bar{X}^2+\bar{X}$	$\{\bar{0}\}$

- $(\bar{X}^2+\bar{X})(\bar{X}^2+\bar{1}) = \bar{X}^4 + \bar{X}^3 + \bar{X}^2 + \bar{1} = \bar{X}^2+\bar{1}$

Lemma:

R endlich. Sei $a \in R$ mit $a \neq 0$.

$\Rightarrow$ a ist entweder Nullteiler oder Einheit.

D.h. $R = R^* \cup R^0 \cup \{0\}$ bzw. $R^c = \{0\}$.

Bew.:

Beh.: a kein Nullteiler, $a \neq 0 \Rightarrow a \in R^*$

Idee: Betrachte $\varphi_a : R \xrightarrow{\cdot a} R$ ein Ring-Hom.

$r \longmapsto r \cdot a$

a kein Nullteiler $\Leftrightarrow$ aus $r \cdot a = 0$ (= $\varphi(r)$) folgt $r = 0$

$\Leftrightarrow \varphi$ injektiv

R endlich $\Rightarrow \varphi_a : R \xrightarrow{\sim} R$ auch surjektiv $\Rightarrow \exists\, s \in R$:

$s \longmapsto 1$

$\varphi(s) = 1$ (= $s \cdot a$)

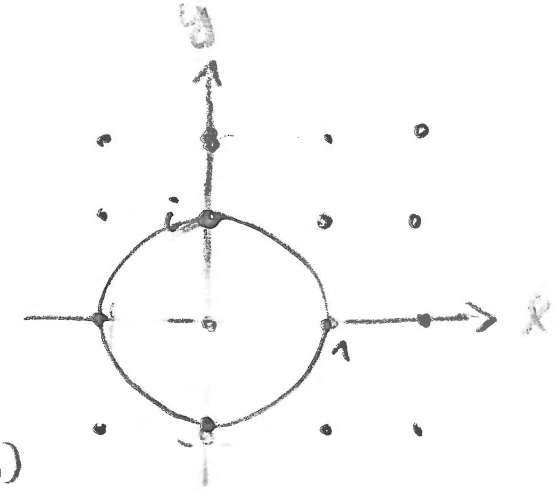
$\Rightarrow$ a eine Einheit.

Corollar: Jeder endliche Integritätsring ist ein Körper.

Zwei Ring-Erweiterungen von $\mathbb{Z}$

(A) Gauß'sche Zahlen

$$\mathbb{Z} \subset \underbrace{\mathbb{Z}+i\mathbb{Z}}_{\{a+ib \mid a,b\in\mathbb{Z}\}} \subset \mathbb{C}$$



$z \in \mathbb{Z}+i\mathbb{Z}$

$$\Rightarrow |z|^2 = z\cdot\overline{z} = (a+ib)(a-ib) = a^2+b^2$$

$(\mathbb{Z}+i\mathbb{Z})^*$ ist endlich

z

$$\Rightarrow \exists z^{-1}: z\cdot z^{-1}=1 \Rightarrow |z\cdot z^{-1}|^2 = 1 \Rightarrow |z|=1$$

$$\Rightarrow (\mathbb{Z}+i\mathbb{Z})^* = \{1, -1, i, -i\} = \langle i\rangle \cong \mathbb{Z}_4$$

i^4 i^2 i^3

$|z|^2 = |z|^2\cdot|z^{-1}|^2$

a^2+b^2 Kreisgleichung

Bem.: $(\mathbb{Z}+i\mathbb{Z})^*$ = ganzzahlige Lösungen der Kreis-Gleichung $x^2+y^2=1$.

(B) $\mathbb{Z}+\sqrt{3}\mathbb{Z} = \{a+\sqrt{3}b \mid a,b\in\mathbb{Z}\}$

- ist $\mathbb{Z}+\sqrt{3}\mathbb{Z}$ ein Ring? a) nullteilerfrei? b) ist $(\mathbb{Z}+\sqrt{3}\mathbb{Z})^*$ endlich? c)

a) $\mathbb{Z}+\sqrt{3}\mathbb{Z} \subset \mathbb{R}$. Seien $a,b,c,d\in\mathbb{Z}$ Beh.: $z,w\in R_3$

$$(a+\sqrt{3}b) + (c+\sqrt{3}d) = (a+c) + \sqrt{3}(b+d)$$

z w $\in\mathbb{Z}$ $\in\mathbb{Z}$

$\Rightarrow z+w$, $z\cdot w \in R_3$.

$$(a+\sqrt{3}b)\cdot(c+\sqrt{3}d) = (ac+3bd) + \sqrt{3}(ad+bc)$$

$\in\mathbb{Z}$ $\in\mathbb{Z}$

$\Rightarrow \mathbb{Z}+\sqrt{3}\mathbb{Z}$ ist Unterring von $\mathbb{R}$

b) sei oben $ac+3bd=0=ad+bc$. Gilt dann $a=b=0$ oder $c=d=0$?

[schwer]. nullteilerfrei!

aber $\mathbb{Z}+\sqrt{3}\mathbb{Z} \subset \mathbb{R}$ $\Rightarrow R_3$ ist IR.

c) Definiere $N: \mathbb{Z}+\sqrt{3}\mathbb{Z} \longrightarrow \mathbb{N}_0$

$$a+\sqrt{3}b \longmapsto |a^2-3b^2|$$

$$z \qquad\qquad z\cdot\bar{z}$$

dann gilt: $N(z)\cdot N(w) = N(z\cdot w) \geq N(z)$ [multiplikativ]

sei $z \in R_3^*$ $\Rightarrow \exists w \in R_3 : z\cdot w = 1$

$\Rightarrow$ $N(z\cdot w) = N(1) = 1$

$\Rightarrow N(z) = 1$

$N(z)\,N(w)$

Lemma: $R_3^* = \{z \in R_3 \mid N(z) = 1\}$.

$\rightarrow$

„$\subseteq$": oben

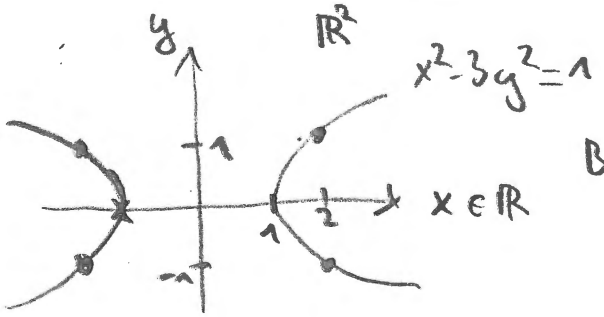
„$\supseteq$": $N(z)=1 = a^2-3b^2 = (a+\sqrt{3}b)\underbrace{(a-\sqrt{3}b)}_{z^{-1}}$ $\quad z=a+\sqrt{3}b$

$\Rightarrow z^{-1} = \bar{z}$.

$\Rightarrow R_3^* =$ ganzzahlige Lösungen der Gleichung

$a^2-3b^2=1$ „Pell / Brouncker - Gleichung"

[Zahlentheorie]



Bem.: $z \in R_3^*$

$\Rightarrow z^n \in R_3^*$ $\quad [(R_3^*, \cdot)$ Gruppe$]$

Fundamentallösung": $a=2 \quad b=1$, $z = 2+\sqrt{3}$

$\Rightarrow \langle z \rangle = \{z^n \mid n \in \mathbb{N}^+\} \cup \{e\} \subset R_3^*$

Beh.: $|\langle z \rangle| = \infty$ $\quad [z^k = z^n \overset{k<n}{\Rightarrow} z^{n-k}(1-z^k)=0]$

Ang.: $|\langle z \rangle| < \infty \Rightarrow \exists k \in \mathbb{N}^+ : z^k = 1$ aber $z \in \mathbb{R}$

$\Rightarrow z \in \{-1, +1\}$. ↯

Bem.: $\langle z \rangle = R_3^*$, $\Rightarrow$

$\mathbb{Z}$

Polynomring

R Ring $\rightsquigarrow$ $R[X] = \{ \sum_{i=1}^{n} a_i X^i \mid a_i \in R,\ n \in \mathbb{N}_0 \}$

$\deg \downarrow$ $\qquad$ $\downarrow (a_n \neq 0)$

$\mathbb{N}_0 \qquad n \qquad \deg(0) := -\infty$

Lemma: R ein NR. $\forall f, g \in R$:

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Bew.: Sei $f(X) = \sum_{i=0}^{n} a_i X^i$ mit $a_n \neq 0$, $g(X) = \sum_{j=0}^{m} b_j X^j$ mit $b_m \neq 0$

$$\Rightarrow g(X) \cdot f(X) = \sum_{k=0}^{m+n} c_k X^k \qquad c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$$

$$\Rightarrow c_{m+n} = a_n \cdot b_m \neq 0 \quad \text{wenn}$$

$\deg(f) = n \Rightarrow a_n \neq 0$

$\deg(g) = m \Rightarrow b_m \neq 0 \Rightarrow c_{m+n} \neq 0 \Rightarrow$

Folgerung: Sei R ein IR

Dann ist auch $\underbrace{R[X] \text{ ein IR}}_{a)}$ und $\underbrace{R[X]^* = R^*}_{b)}$.

Bew.:

a) Seien $f, g \in R[X] \setminus \{0\}$ mit $f(X) \cdot g(X) = 0$

$$\Rightarrow \deg(f \cdot g) = \deg(0) = -\infty$$

$$\| \qquad (m=0) \quad (n=0)$$

$$\deg(f) + \deg(g) \Rightarrow f(X) = a_0 \quad g(X) = b_0$$

$$\Rightarrow a_0 \cdot b_0 = 0 \Rightarrow f = a_0 = 0$$

R NR $\quad g = b_0 = 0$

b) Sei $f \cdot g = 1$

$$\Rightarrow \deg(f) + \deg(g) = \deg(f \cdot g) = \deg(1) = 0$$

$$\Rightarrow \deg(f) = \deg(g) = 0 \Rightarrow f(X) = a_0 \quad g(X) = b_0 \quad a_0 b_0 = 1$$

$f \in R^*$

$\Uparrow$

Polynomring vs. Potenzreihenring

$R = K$

$$K[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid a_i \in K \right\} = \left\{ \sum_{i=0}^{\infty} a_i X^i \mid a_i \in K, \text{ aber nur endlich viele } a_i \neq 0 \right\}$$

$$\downarrow$$

$$K[[X]] = \left\{ \sum_{i=0}^{\infty} a_i X^i \mid a_i \in K \right\}$$

z.B. $\sum_{i=0}^{\infty} 2^i \cdot x^i$

R	R^*	R^0	R^c	
$K[X]$	a_0 mit $a_0 \neq 0$	$\emptyset$	$\sum_{i=1}^{n} a_i X^i$	} Euklidische Ringe
$K[[X]]$	$\sum_{i=0}^{\infty} a_i X^i$ mit $a_0 \neq 0$	$\emptyset$	$\sum_{i=1}^{\infty} a_i X^i$	

Bem.: $f \in K[X]$ mit $f(0) \neq 0$ $\Leftrightarrow$ $\exists$ genau ein $f^{-1} \in K[[X]] \setminus K[X]$

$f^{-1} \cdot f = 1$.

Zusammenfassung

Körper $\subset$ (Konvention) euklidische Ringe $\subset$ Hauptidealringe $\subset$ Ringe

$\mathbb{Q}$	$\mathbb{Z}$	$R[X]$ wenn R ein HIR		$C^0(\mathbb{R})$, $C^\infty(\mathbb{R})$
$\mathbb{R}$	$K[X]$, $K[[X]]$	$[K[X], Y]$		$K[X]/(f \cdot g)$
$\mathbb{C}$	$R_{-1} = \mathbb{Z} + i\mathbb{Z}$	$R_{-19} = \mathbb{Z} + \frac{1+\sqrt{-19}}{2}\mathbb{Z}$		$\deg(f), \deg(g) \geq 1$
	$R_3 = \mathbb{Z} + \sqrt{3}\mathbb{Z}$			

$\mathbb{R}[X]$

endl. Körper = endl. euklid. Ringe = endl. HIR $\subset$ endliche Ringe

$\mathbb{Z}_p$ | $\mathbb{Z}_{m \cdot n}$ | $\mathbb{Z}_p[X]/(X^n)$

Tutorium #7: 19.12.2014

Faktorringe, Euklidischer Algorithmus und simultane Kongruenzen

① Rechnen mit Restklassen

R Ring, $I \subset R$ ein Ideal

$\rightsquigarrow R/I = \{r + I \mid r \in R\}$ ein Faktorring

$(r_1 + I) + (r_2 + I) := (r_1 + r_2) + I \quad \rightsquigarrow \quad \overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$

$(r_1 + I) \cdot (r_2 + I) := (r_1 \cdot r_2) + I \quad \rightsquigarrow \quad \overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2}$

Notation: $r + I = \overline{r}$ oder $[r]$ (oder wieder „r"!)

Bsp. 1: $R = \mathbb{Z} \quad I = 5\mathbb{Z} = (5)$

$\rightsquigarrow R/I = \mathbb{Z}/(5) =: \mathbb{Z}_5 \qquad \mathbb{Z}_5 = \{k + 5\mathbb{Z} \mid k \in \mathbb{Z}\}$

- $\overline{5} + 5\mathbb{Z} = 0 + 5\mathbb{Z} \rightsquigarrow \overline{5} = \overline{0}$
- rechne in $\mathbb{Z}_5$ wie in $\mathbb{Z}$ aber $\overline{5} = \overline{0}$,

z.B. $(2 + 5\mathbb{Z}) \cdot (3 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = (1 + \underbrace{5\mathbb{Z}}_{=5\mathbb{Z}}) + (0 + 5\mathbb{Z}) = 1 + 5\mathbb{Z}$

$\rightsquigarrow \overline{2} \cdot \overline{3} = \overline{6} = \overline{1} + \overline{5} = \overline{1}$ oder $2 \cdot 3 \equiv 1 \mod 5$

$\Rightarrow \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{5}, \overline{-4}, \overline{7}, \overline{8}, \overline{14}\} \ldots$

Bsp. 2: $R = K[x] \quad f(x) = x^2 + 1 \quad I = (f)$

$\rightsquigarrow R/I = K[x]/(x^2+1)$ [manchmal „$K[x]/x^2+1$"]

$= \{p(x) + (x^2+1) \mid p \in K[x]\}$

- $x^2 + 1 + I = x^2 + 1 + (x^2+1) = 0 + (x^2+1) \rightsquigarrow \overline{x^2+1} = \overline{0}$

oder $x^2 + I = x^2 + 1 - 1 + I = -1 + I \rightsquigarrow \overline{x^2} = \overline{-1}$

- rechne in $K[x]/I$ wie in $K[x]$ aber $\overline{x}^2 = \overline{-1}$

z.B. $\overline{2x-1} \cdot \overline{(x+2)} = \overline{2x^2 - x + 4x - 2} = \overline{2x^2 + 3x - 2}$

$= \underbrace{2x^2 + 2 - 2}_{\in I} + 3x - 2 + I = 3x - 4 + I = \overline{3x-4}$

$\rightsquigarrow \overline{2x^2+3x-2} = \overline{2(-1) + 3x - 2} = \overline{3x-4}$

Beh.: $K[X]/(X^2+1) = \{\overline{a+bx} \mid a,b \in K\}$ (*)

„$\supseteq$": ✓

„$\subseteq$": Sei $\bar{p} \in K[X]/(X^2+1)$

$$\Rightarrow \overline{p(X)} = \sum_{j=0}^{n} \overline{a_j X^j} = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \overline{a_{2j} X^{2j}} + \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \overline{a_{2j+1} X^{2j+1}}$$

$$= \underbrace{\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \overline{(-1)^j \cdot a_{2j}}}_{\bar{a}} + \underbrace{\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \overline{(-1)^j a_{2j+1}} \cdot \bar{x}}_{\bar{b}}, \text{ denn } \overline{x^{2j}} = (\overline{x^2})^j = (\overline{-1})^j.$$

② $\mathbb{C}$ als Faktorring

Lemma: $\mathbb{R}[X]/(X^2+1) \xrightarrow[\bar{\varphi}]{\sim} \mathbb{C}$, d.h. $\bar{\varphi}$ wohldef. & Ring-Isom.

$$\overline{a+bx} \longmapsto a+b\cdot i$$

Insbesondere ist $\mathbb{R}[X]/(X^2+1)$ ein Körper.

Beweis: Betrachte $\varphi: \mathbb{R}[X] \longrightarrow \mathbb{C}$ $\quad \varphi(p(X)) = p(i)$

also $p(X) = \sum_{j=0}^{n} a_j X^j \longmapsto \sum_{j=0}^{n} a_j i^j$ ein Ring-Hom.

a) Beh.: $(X^2+1) \subset \ker \varphi$:

$$\varphi(p(X) \cdot (X^2+1)) = \varphi(p(X)) \cdot \varphi(i^2+1) = 0$$

$$\Rightarrow \quad \begin{array}{ccc} \mathbb{R}[X] & \xrightarrow{\varphi} & \mathbb{C} \\ & \searrow^{\pi} & \uparrow_{\bar{\varphi}} \\ & & \mathbb{R}[X]/(X^2+1) \end{array} \qquad \exists \bar{\varphi}: \ \bar{\varphi} \cdot \pi = \varphi$$

$$\bar{\varphi}(\overline{a+bx}) = \varphi(a+bx) = a+bi$$

b) Beh.: φ surjektiv. Sei $a+bi \in \mathbb{C} \Rightarrow a+bi = \varphi(a+bx)$

$\Rightarrow \bar{\varphi}$ surjektiv

c) Beh.: $\bar{\varphi}$ injektiv.

Sei $\bar{p} \in \ker \bar{\varphi}$. $\overset{(*)}{\Rightarrow} \overline{p(X)} = \overline{a+bx}$ mit $a,b \in \mathbb{R}$

$\Rightarrow \bar{\varphi}(\bar{p}(X)) = 0 = a+ib \Rightarrow a=b=0 \Rightarrow \bar{p} = \bar{0}$. □

③ Der Euklidische Algorithmus

Sei $R = \mathbb{Z}$ oder $K[X]$

Sätze: 1) R ist Euklidisch, [wobei $N: R \longrightarrow \mathbb{N}_0^+$

$a \longmapsto \begin{cases} |a| & R=\mathbb{Z} \\ \deg(a) & R=K[X] \end{cases}$]

$\Rightarrow$ 2) R ist Hauptidealring

$\Rightarrow$ 3) jedes Element $r \in R \setminus \{0\}$ hat eine Primfaktorzerlegung

Seien $a, b \in R \overset{2)}{\Rightarrow} \exists r \in R: (a,b) = (\underbrace{r}_{ggT(a,b)})$ [R ist „faktoriell"]

$\Rightarrow \exists u, v \in R: u \cdot a + v \cdot b = r$

Euklid. Algorithmus $\Rightarrow ggT(a,b)$ sowie u und v

PFZ von a & b $\Rightarrow$ nur $ggT(a,b)$]

Algorithmus

$a, b \in R \setminus \{0\}$

„a / b" $\exists q_1, r_1 \in R$ mit $N(b) > N(r_1)$

und $a = q_1 b + r_1$

„b / r_1" $\exists q_2, r_2 \in R$ ...

$b = q_2 r_1 + r_2$

„r_1 / r_2" $\exists q_3, r_3$: $r_1 = q_3 r_2 + r_3$

$\vdots$

$\exists n \in \mathbb{N}$:

„r_{n-1} / r_n" $r_{n-1} = q_{n+1} r_n + 0$

$\Rightarrow ggT(a,b) = r_n$

Löse Gleichungen nach r_n auf $\Rightarrow u$ und v.

Bsp.: $R = \mathbb{Z}$ [optional]

$a = 1071 \quad b = -1029$

$1071 = (-1) \cdot (-1029) + 42$

$-1029 = (-24) \cdot 42 + 21$

$42 = 2 \cdot 21 + 0$

$\Rightarrow ggT(a,b) = 21$

$\cdot 21 = -1029 - (-24) \cdot 42$

$ggT(a,b) = -1029 - (-24)[1071 - 1029)$

$= 24 \cdot 1071 - 25 \cdot 1029$

$u \quad a \quad v \quad b$

Bem.: $1071 = 3 \cdot 357 = 3 \cdot 7 \cdot 51 = 3^2 \cdot 7 \cdot 17$

$1058 = 3 \cdot 342 = 3 \cdot 7 \cdot 49 = 3 \cdot 7^3$ $\Rightarrow ggT(a,b) = 3 \cdot 7.$

Aufg.

$f(x) = x^3 - 1, \quad g(x) = x^3 - 3x^2 + 5x - 3 \quad \in \mathbb{Q}[x] = R$

Bestimme $ggT(f, g)$.

Euklid. Algorithmus.

$\exists$

"g" $\exists q_1, r_1 \in R : \deg(f) > \deg(r_1)$

$g = q_1 f + r_1$

"f" $\exists q_2, r_2 \dots$

$f = q_2 r_1 + r_2$

"r_1" $\exists q_3, r_3 :$

$r_1 = q_3 r_2 + r_3$

$\vdots$

$\exists n \in \mathbb{N} :$

"r_{n-1}" $r_{n-1} = q_{n+1} r_n + 0$

$\Rightarrow ggT(f, g) = r_n$

Bsp.:

g $\quad$ f

$(x^3 - 3x^2 + 5x - 3) : (x^3 - 1) = \underbrace{1}_{q_1}$

$-(x^3 - 1)$

$\underbrace{-3x^2 + 5x - 2}_{r_1}$

$f \quad r_1$

$(x^3 - 1) : (-3x^2 + 5x - 2) = \underbrace{-\frac{1}{3}x - \frac{5}{9}}_{q_2}$

$-(x^3 - \frac{5}{3}x^2 + \frac{2}{3}x)$

$\frac{5}{3}x^2 - \frac{2}{3}x - 1$

$-(\frac{5}{3}x^2 - \frac{25}{9}x + \frac{10}{9})$

$\underbrace{\frac{25-6}{9}x - \frac{19}{9}}_{r_2}$

$r_1 \quad r_2$

$(-3x^2 + 5x - 2) : (\frac{19}{9}x - \frac{19}{9})$

$= \frac{9}{19} \cdot [(-3x^2 + 5x - 2) : (x - 1)] = \underbrace{\frac{9}{19} \cdot [-3x + 2]}_{q_3}$

$-(-3x^2 + 3x)$

$2x - 2$

$2x - 2$

$\underbrace{0}_{r_3}$

$\Rightarrow ggT(f, g) = r_2(x) = \frac{19}{9}(x - 1)$

oder $(x - 1)$.

---

em.: $PFZ(f) = (x-1) \cdot \underbrace{(x^2 + x + 1)}_{\text{irreduzibel in } \mathbb{Q}[x]} \Rightarrow ggT(f, g) = (x - 1).$

$PFZ(g) = (x-1) \cdot (x^2 - 2x + 3)$

Aufg.:

$f(x) = x^2+x+1$

$g(x) = x^2-2x+3 \in \mathbb{Q}[x]$.

Ist $\bar{g}$ invertierbar in $\mathbb{Q}[x]/(f)$? Wenn ja, was ist $\bar{g}^{-1}$?

Satz: $\bar{g}$ inv. in $\mathbb{Q}[x]/(f) \Leftrightarrow ggT(f,g)=1$.

Beweis: $\bar{g}$ inv. in $\mathbb{Q}[x]/(f)$

$\Leftrightarrow \exists \bar{v} \in \mathbb{Q}[x]/(f): \bar{g}\bar{v} = \bar{1} \Leftrightarrow \exists \bar{v} \in \mathbb{Q}[x]/(f): \overline{gv-1} = \bar{0}$

$\Leftrightarrow \exists v \in \mathbb{Q}[x]: gv-1 \in (f) \Leftrightarrow \exists u,v \in \mathbb{Q}[x]: gv-1 = u\cdot f$

$\Leftrightarrow \exists u,v \in \mathbb{Q}[x]: (-u)\cdot f + gv = 1 \Leftrightarrow ggT(f,g)=1$

• in diesem Fall ist $\bar{g}^{-1} = \bar{v}$.

Bsp.:

g | $(x^2-2x+3):(x^2+x+1) = 1$ | q_1
f | $-(x^2+x+1)$
| $-3x+2$

$g = q_1 f + v_1$

$f = q_2 v_1 + v_2$

f | $(x^2+x+1):(-3x+2) = \underbrace{-\frac{1}{3}x - \frac{5}{9}}_{q_2}$
v_1 | $-(x^2-\frac{2}{3}x)$
| $+\frac{5}{3}x+1$
| $-(+\frac{5}{3}x-\frac{10}{9})$
| $\frac{19}{9}$
| $\underbrace{\quad}_{v_2}$

$\Rightarrow v_2 = f - q_2 v_1$

$= f - q_2(g - q_1 f)$

$= -q_2 g + (\ldots) f$

$\Rightarrow \bar{v}_2 = \overline{-q_2 g}$ in $\mathbb{Q}[x]/(f)$

$\Rightarrow \frac{\bar{19}}{9} = \overline{(\frac{1}{3}x+\frac{5}{9})} \cdot \bar{g}$

$\Rightarrow \bar{g}^{-1} = \overline{\frac{9}{19}(\frac{1}{3}x+\frac{5}{9})} = \overline{\frac{1}{19}(3x+5)}$ □.

④ Simultane Kongruenzen

Chinesischer Restsatz für $\mathbb{Z}$:

Seien $m_1, \dots, m_n \in \mathbb{Z}$ paarweise teilerfremd.
[d.h. $ggT(m_i, m_j) = 1 \ \forall i \neq j$].
Sei $m = m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Dann gilt:

$$\mathbb{Z}_m \xrightarrow[\psi]{\sim} \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_n}$$

$$x + (m) \longmapsto (x + (m_1), x + (m_2), \dots, x + (m_n))$$

$$\| \quad \bar{x} \longmapsto (\bar{x}, \bar{x}, \dots, \bar{x})''$$

Anwendung: Sei $n = 3$. Seien $a_1, a_2, a_3 \in \mathbb{Z}$ gegeben.
Suche alle $x \in \mathbb{Z}$ mit

mit
$$\left.\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ x &\equiv a_3 \bmod m_3 \end{aligned}\right\} (*)$$

Bsp.:
$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 4 \\ x &\equiv 1 \bmod 5 \end{aligned}$$

Bem.: a) falls x eine Lsg von $(*)$ ist, so auch $x + m \cdot k \ \forall k \in \mathbb{Z}$
[$x + 60k$]

$\rightsquigarrow$ suche eine Lsg. $\bar{x} \in \mathbb{Z}_m$.

b) [CRS] $\Rightarrow \mathbb{Z}_{60} \xrightarrow[\psi]{\sim} \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \Rightarrow \exists! \bar{x} \in \mathbb{Z}_{60}$ so dass

$\exists! \bar{x} \longmapsto (\bar{2}, \bar{3}, \bar{1})$

$\|$ $\quad \|$ $\quad \|$

$(x + (60)) \quad (2 + (3), 3 + (4), 1 + (5))$

x = das Gleichungssystem $(*)$ löst.

Wie findet man x?

1) $60 = 3 \cdot 20 = 4 \cdot 15 = 5 \cdot 12$

$m \quad a_1 \ b_1 \quad a_2 \ b_2 \quad a_3 \ b_3$ $\quad \| \ a_i u_i + b_i v_i = 1''$

$ggT(3,20) = 1 \Rightarrow \exists u_1, v_1 \in \mathbb{Z}: \ 3u_1 + 20v_1 = 1$ $\rightsquigarrow$ Finde

$ggT(4,15) = 1 \Rightarrow \dots \quad 4u_2 + 15v_2 = 1$ u_1, v_1

$ggT(5,12) = 1 \Rightarrow \dots \quad 5u_2 + 12v_2 = 1$ $\dots u_3, v_3$.

Euklid. Alg. 1.

$3 \cdot 7 + 20 \cdot (-1) = 1$

$\Rightarrow \quad 4 \cdot 4 + 15 \cdot (-1) = 1$

$5 \cdot 5 + \underbrace{12 \cdot (-2)}_{e_i = b_i v_i} = 1$

Sehe $e_1 = -20$, $e_2 = 15$, $e_3 = -24$

Dann gilt: $e_i \equiv \begin{cases} 1 \mod m_i & i = j \\ 0 \mod m_j & i \neq j \end{cases}$ z.B. $e_1 \equiv \begin{cases} 1 \mod 3 \\ 0 \mod 4 \\ 0 \mod 5 \end{cases}$ $\quad = -20$

Sehe $\overline{x} = \sum_{i=1}^{n} a_i e_i + (m) \in \mathbb{Z}_m$. Dann gilt $x \equiv a_i \mod m_i$!

$= a_1 e_1 + a_2 e_2 + a_3 e_3 + (m)$

$= 2 \cdot (-20) + 3 \cdot (-15) + 1 \cdot (-24) + 60\mathbb{Z}$

$\Rightarrow \quad x \equiv -40 - 45 - 24 \mod 60$

$\equiv -109 \mod 60$

$\equiv 11 \mod 60$

Test: $11 \equiv 2 \mod 3$

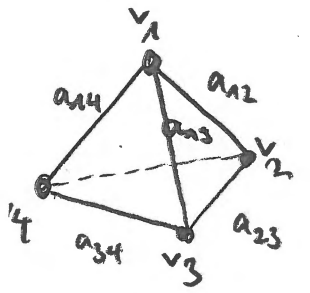
$11 \equiv 3 \mod 4$

$11 \equiv 1 \mod 5$ ✓.

Tutorium #8 08.01.2015

Lösung der Aufgaben zur Wiederholung

Aufg. 1:



Färbe Ecken und Kanten eines Tetraeders T in gelb oder blau.
Wieviele Färbungen bis auf Drehung von T gibt es?

1) Formulierung einer Gruppen-Wirkung:

Drehgruppe von $T = A_4$

M = alle möglichen Färbungen von T

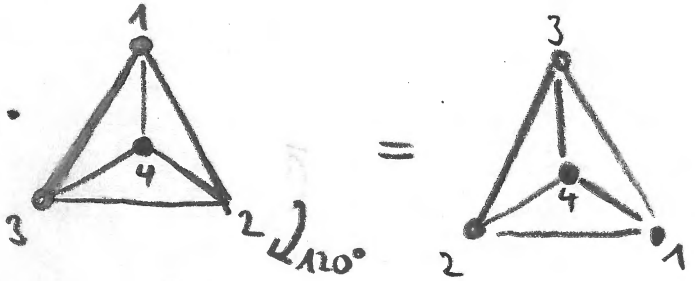
$= \{(v_1, v_2, v_3, v_4, a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{34}) \mid v_i, a_{ij} \in \{\text{gelb, blau}\}\}$

$i, j \in \{1,2,3,4\}$.

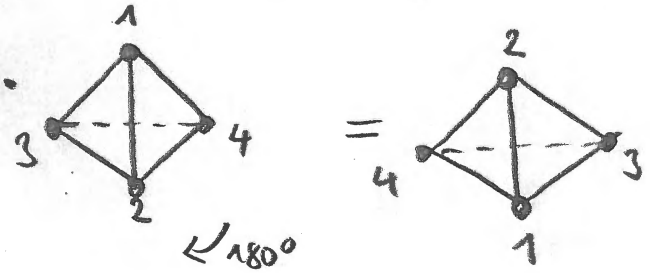
$\Rightarrow$ $A_4 \times M \longrightarrow M$ eine Gruppenwirkung

$\sigma \cdot (v_1, \dots, a_{34}) = (v_{\sigma(1)}, \dots, a_{\sigma(3)\,\sigma(4)})$

z.B.: $\sigma = (123)$ ·



oder $\tau = (12)(34)$ ·



2) Konjugations-Klassen von A_4:

$A_4 = \{e\} \dot\cup \{\overbrace{(12)(34)}^{\tau}$
$(14)(23)$
$(13)(24)\} \dot\cup \{\overbrace{(123)}^{\sigma},$
$(124),$
$(234)\}$
(134)
$\dot\cup \{\overbrace{(132)}^{\sigma^2}$
$(142),$
$(243)\}$
(143)

c) Bahnformel:

Tetraeder bis auf Drehung (gefärbte) = # der Bahnen

$= \#\, M/A_4 = \frac{1}{|A_4|} \sum_{g \in A_4} \chi(g)$ $\qquad \chi(g) = \#\,\underbrace{\mathrm{Fix}(g)}_{\{m \in M \mid gm = m\}}$

$g \sim h \Rightarrow \chi(g) = \chi(h)$

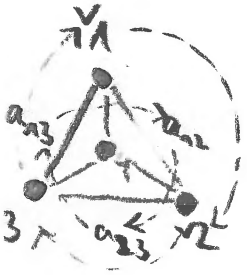
↳ bestimme $\chi(\sigma)$, $\chi(\sigma^3)$, $\chi(\tau)$.

• $g = \sigma$: sei $m \in M$ mit $\sigma(m) = m$

$m = (v_1, v_2, v_3, v_4, a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{34})$

$= \sigma(m) = (v_{\sigma(1)}, \dots, v_{\sigma(4)}, a_{\sigma(1)\sigma(2)}, \dots, a_{\sigma(3)\sigma(4)})$ $\qquad \sigma = (123)$

$= (v_2, v_3, v_1, v_4, a_{23}, a_{21}, a_{24}, a_{31}, a_{14})$



$\Rightarrow v_1 = v_2 = v_3$

$a_{12} = a_{23} = a_{13} \qquad a_{14} = a_{24} = a_{34}$

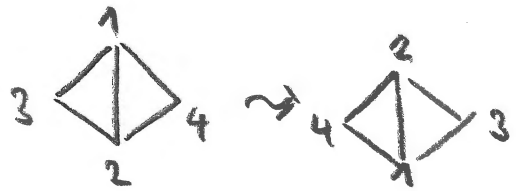
v_4, bel.

$\Rightarrow \chi(\sigma) = 2^4$

$g = \sigma^2$ analog $\Rightarrow \chi(\sigma^2) = 2^4$

$g = e$: $\chi(e) = \#M = 2^{10}$ (4 Ecken & 6 Kanten)

$g = \tau = (12)(34)$:



$m \in \mathrm{Fix}(\tau) \Rightarrow v_1 = v_2 \quad v_3 = v_4 \quad a_{13} = a_{24} \quad a_{14} = a_{23}$

a_{34}, a_{12} bel.

$\Rightarrow \chi(\tau) = 2^6$

$\Rightarrow \#M_{A_4} = \frac{1}{12}(\chi(e) + 4\chi(\sigma) + 4\chi(\sigma^2) + 3\chi(\tau))$

$= \frac{1}{12}(2^{10} + 4 \cdot 2^5 + 3 \cdot 2^6) = \frac{2^5}{12}(32 + 4 + 6) = \frac{8}{3} \cdot 42 = 8 \cdot 14 = 112.$

Aufg. 2: G Gruppe mit $|G| = 1000$.

G auflösbar?

$1000 = 10^3 = 2^3 \cdot 5^3 = 8 \cdot 125$

verwende Sylow-Satz 3: $|G| = p^k \cdot m$ mit p prim, $ggT(p,m) = 1$

$n_p = \#$ p-Sylow-UG in G $\Rightarrow \begin{cases} n_p \equiv 1 \bmod p \\ n_p \mid m \end{cases}$

[a) $p=2$: $1000 = 2^3 \cdot 125 \Rightarrow \begin{cases} n_2 \equiv 1 \bmod 2 \\ n_2 \mid 125 \end{cases} \Rightarrow n_2 \in \{1, 5, 25, 125\}$

~~oder~~

$\rightsquigarrow$ nicht aufschlussreich]

b) $p=5$: $1000 = 5^3 \cdot 8 \Rightarrow \begin{cases} n_5 \equiv 1 \bmod 5 \\ n_5 \mid 8 \end{cases} \Rightarrow n_5 \in \{1, \cancel{2}, \cancel{4}, \cancel{8}\}$

$n_5 = 1$

$\Rightarrow \exists!$ 5-Sylow-UG H in G. $\Rightarrow H$ ist normal, also $H \triangleleft G$

[$n_p = 1 = \frac{|G|}{|N_G(H)|} \Leftrightarrow |N_G(H)| = |G| \Leftrightarrow H \triangleleft G$].

jede p-Gruppe ist auflösbar, also auch H.

$|G/H| = \frac{1000}{125} = 8 = 2^3 \Rightarrow G/H$ auflösbar

$H \triangleleft G$, G/H auflösbar $\Rightarrow G$ auflösbar

Aufg. 3:

$G' = [G,G] \subset N \subset G$ Normalteiler $N \triangleleft G$.

Kommutatorgruppe

Aufg. 3:

$N \subset G$ UG so dass $G' = [G,G] \subset N \subset G$.

Beh.: $N \triangleleft G$. [Es gibt elementare Lösung: siehe Seite ⑥]

Bew.:

verwende Korrespondenzsatz auf $G \xrightarrow{\pi} G^{ab} = G/_{[G,G]}$ an

$\Rightarrow$ es gibt Bijektion

$$\{N \mid [G,G] \subset N \subset G \text{ UG}\} \xleftrightarrow{1:1} \{H \mid H \subset G^{ab} \text{ UG}\}$$
$$N \longmapsto \pi(N)$$

wobei $N \triangleleft G \Leftrightarrow \pi(N) \triangleleft G^{ab}$

- G^{ab} abelsch $\Rightarrow H \triangleleft G^{ab}$ für alle $H \subset G$ UG

$\Rightarrow \pi(N) \triangleleft G^{ab} \Rightarrow N \triangleleft G$. □

Aufg. 4: finde kleinstes $x \in \mathbb{N}$ mit

$$(*) \begin{cases} x \equiv 2 \bmod 5 & x \equiv a_1 \bmod m_1 \\ x \equiv 3 \bmod 8 & x \equiv a_2 \bmod m_2 \\ x \equiv 4 \bmod 7 & x \equiv a_3 \bmod m_3 \end{cases}$$

Chin. Restsatz $\Rightarrow \exists! \bar{x} \in \mathbb{Z}_m$ das $(*)$ löst.

$$m = 5 \cdot 8 \cdot 7 = 40 \cdot 7 = 280 = m_1 \cdot m_2 \cdot m_3$$

- $280 = 5 \cdot 56 = 8 \cdot 35 = 7 \cdot 40$

		a_i v_i	
$\text{ggT}(5,56)=1$	$\Rightarrow \exists a_1, b_1 \in \mathbb{Z}$: u_1 v_1	$5a_1 + 56b_1 = 1$	z.B. $5 \cdot (-11) + 56 = 1$
$\text{ggT}(8,35)=1$		$8a_2 + 35b_2 = 1$	$8 \cdot (-13) + 35 \cdot 3 = 1$
$\text{ggT}(7,40)=1$		$7a_3 + 40b_3 = 1$	$7 \cdot (-17) + 40 \cdot 3 = 1$

setze $e_1 = 56b_1 = 56 \quad e_2 = 35 \cdot 3 = 105 \quad e_3 = 40 \cdot 3 = 120$

$$\Rightarrow e_i \equiv \begin{cases} 1 \bmod m_i \\ 0 \bmod m_j \end{cases} \quad i \neq j$$

$\Rightarrow x = \sum a_i e_i = 2e_1 + 3e_2 + 4e_3 \equiv 112 + 315 + 480 \bmod 280$ ④

$\equiv 112 + 35 + 200 \bmod 280 \equiv 347 \bmod 280 \Rightarrow x = 67$ □

Aufg. 5

$f(x) = x^3 - 3x - 2$

$g(x) = 2x^3 - 4x^2 - 10x + 12 \quad \in \mathbb{Q}[x]$

Ist $\bar{g}$ invertierbar in $\mathbb{Q}[x]/(f)$? Wenn ja, was ist $\bar{g}^{-1}$?

Sem.: $\bar{g}$ invertierbar in $\mathbb{Q}[x]/(f) \Leftrightarrow ggT(f,g) = 1$

$\Leftrightarrow$

In diesem Fall: $\exists u, v: \; u \cdot f + v g = 1$

$\Rightarrow \bar{g}^{-1} = v.$

ow.: $\bar{g}$ inv. in $\mathbb{Q}[x]/(f) \Leftrightarrow \exists \bar{v} \in \mathbb{Q}[x]/(f): \; \bar{v} \cdot \bar{g} = \bar{1}$

$\Leftrightarrow$ " $\quad\quad vg - 1 = \bar{0}$

$\Leftrightarrow \exists v \in \mathbb{Q}[x]: \quad vg - 1 \in (f)$

$\Leftrightarrow \exists u, v \in \mathbb{Q}[x]: \; -u \cdot f + v \cdot g = 1$

$\Leftrightarrow ggT(f,g) = 1$ und $\bar{g}^{-1} = \bar{v}$

Berechne $ggT(f,g)$ mit Euklid.-Algorithmus:

f / g: $(x^3 - 3x - 2) : (2x^3 - 4x^2 - 10x + 12) = \underbrace{\frac{1}{2}}_{q_1}$

$-(x^3 - 2x^2 - 5x + 6)$

$\underbrace{2x^2 + 2x - 8}_{r_1}$

g / r_1: $(2x^3 - 4x^2 - 10x + 12) : (2x^2 + 2x - 8) = \underbrace{x - 3}_{q_2}$

$-(2x^3 + 2x^2 - 8x)$

$-6x^2 - 2x + 12$

$-(-6x^2 - 6x + 24)$

$\underbrace{4x - 12}_{r_2}$

r_1 / r_2: $(2x^2 + 2x - 8) : (4x - 12) = \underbrace{\frac{1}{2}x + 2}_{q_3}$

$-(2x^2 - 6x)$

$8x - 8$

$-(8x - 24)$

$\underbrace{16}_{r_3} \in \mathbb{Q}[x]^* = \mathbb{Q}^*$

r_2 / r_3: $(4x - 12) : 16 = \frac{1}{4}x - \frac{3}{4}$

$\Rightarrow r_4 = 0$

$\Rightarrow ggT(f,g) = 1$

[ggT eindeutig bis auf Einheit]

Bestimmung von $\bar{g}^{-1}$:

$f = q_1 g + r_1$ $\quad \Rightarrow r_3 = r_1 - q_3 r_2 = r_1 - q_3(g - q_2 r_1)$

$g = q_2 r_1 + r_2$ $\quad = r_1(1 + q_2 q_3) - q_3 g$

$r_1 = q_3 r_2 + r_3$ $\quad = (f - q_1 g)(1 + q_2 q_3) - q_3 g$

$r_3 \in \mathbb{Q}^*$ $\quad = (-q_1 - q_1 q_2 q_3 - q_3) g + (\ldots) \cdot f$

$\Rightarrow \bar{r}_3 = \overline{16} = \overline{(-q_1 - q_1 q_2 q_3 - q_3) g}$ in $\mathbb{Q}[X]/(f)$

$\Rightarrow \bar{g}^{-1} = -\frac{1}{16}\overline{(+q_1 + q_1 q_2 q_3 + q_3)}$

$= \frac{1}{16}\left(+\frac{1}{2} + \frac{1}{2}(x-3)\left(\frac{1}{2}x+2\right) + \left(\frac{1}{2}x+2\right)\right)$

$= \frac{1}{16}\left(\frac{1}{2} + \frac{1}{2}\left(\frac{1}{2}x^2 + \frac{1}{2}x - 6\right) + \frac{1}{2}x + 2\right)$

$= \frac{1}{32}\left(1 + \frac{1}{2}x^2 + \frac{1}{2}x - 6 + x + 1\right)$

$= \frac{1}{32}\left(\frac{1}{2}x^2 + \frac{3}{2}x - 4\right) = \overline{\frac{1}{64}(x^2 + 3x - 2)}$. $\square$

Aufg. 3:

$N \subset G$ UG mit $G' = [G, G] \subset N \subset G$.

Beh: $N \trianglelefteq G$ oder $gN = Ng$ $\forall g \in G$ oder $gNg^{-1} \subset N$

[denn $gNg^{-1} \supset N$ mit $g = e$]

Bew.:

Sei $g \in G$ und $n \in N$. Beh.: $gng^{-1} \in N$

$\Rightarrow$ es gilt $gng^{-1}n^{-1} \in G'$ [nach Def. von G']

also $gng^{-1} \in G' \cdot n$

G' ist UG von N und $n \in N$ $\Rightarrow G' \cdot n \subset N$.

$\Rightarrow gng^{-1} \in N$ $\square$