UE 162 ▶ Übungsaufgabe 3.2.4.15. (W) Zeigen Sie ◀ **UE 162**

$$C_n \cong \bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$$

für die zyklische Gruppe C_n der Ordnung $n = \prod_{p\in\mathbb{P}} p^{e_p}$.

·) „$\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$ ist zyklische Gruppe": Als direkte Summe von zyklischen Gruppen ist $\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$ eine Gruppe.

$q\in\mathbb{P}$ bel. $\prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p}\,(1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = \left(\prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p} + p^{e_p}\mathbb{Z}\right)_{p\in\mathbb{P}} = \prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p}\,(f_p(q)+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}$, wobei $f_p(q)=0$, falls $p\neq q$

und $f_p(q)=1$, falls $p=q$; wir erhalten also mit $\ell_q := \prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p} \bmod q^{e_q} \in \{1,\dots,q^{e_q}-1\}$

$\prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p}\,(1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = \ell_q\,(f_p(q)+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}$ Da nach Prop. 3.2.4.9 ℓ_q ein erzeugendes Element von $C_{q^{e_q}}$ ist, gibt es ein $m_q\in\mathbb{N}$ mit $m_q\,\ell_q\,(f_p(q)+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = (f_p(q)+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}$

Also: $m_q \prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p}\,(1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = (f_p(q)+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}$

Für bel. $(k_p+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} \in \bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$ erhalten wir also $(k_p+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = \left(\sum_{q\in\mathbb{P}} k_q\, m_q \prod_{p\in\mathbb{P}\setminus\{q\}} p^{e_p}\right)(1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}$

Also ist $\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}} = \langle (1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}\rangle$ und damit eine zyklische Gruppe.

·) „n-elementig": $n\,(1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = \prod_{p\in\mathbb{P}} p^{e_p}\,(1+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} = (0+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}}$ also ist die $\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$ höchstens n-elementig

Da $(f_p(q)+p^{e_p}\mathbb{Z})_{p\in\mathbb{P}} \in \bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$ sieht man, dass es mindestens $\prod_{p\in\mathbb{P}} p^{e_p} = n$ Elemente geben muss

Als n-elementige zyklische Gruppe ist nach Prop. 3.2.4.7: $\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}} \cong C_n$

Proposition 3.2.5.6. *Sei G eine Gruppe. Für alle $g \in G$ definieren wir $\pi_g \colon G \to G$ $x \mapsto gxg^{-1}$ und betrachten die Abbildung $\Phi : g \mapsto \pi_g$. Dann gilt:*

1. *Für $g, h \in G$ gilt $\pi_g \circ \pi_h = \pi_{gh}$. Somit ist Φ ein Homomorphismus von G in die Automorphismengruppe* $\mathrm{Aut}(G)$.

2. *Für alle $g \in G$ ist π_g ein Automorphismus (genannt der durch* Konjugation *mit g induzierte* innere Automorphismus *von G).*

3. *Für den Kern von Φ gilt*

$$\ker(\Phi) = Z(G) = \{g \in G : \ \forall h \in G : \ gh = hg\}.$$

Insbesondere ist $\Phi \colon G \to \mathrm{Aut}(G)$ eine isomorphe Einbettung genau dann, wenn das Einselement $e \in G$ das einzige ist, das mit allen $g \in G$ vertauscht.

4. *Die inneren Automorphismen bilden einen Normalteiler $\Phi(G) \lhd \mathrm{Aut}(G)$ der Automorphismengruppe von G. (Die Faktorgruppe $\mathrm{Aut}(G)/\Phi(G)$ nennt man auch die* äußere Automorphismengruppe *von G.)*

UE 164 ▶ Übungsaufgabe 3.2.5.7. (W) Beweisen Sie Proposition 3.2.5.6. **◀ UE 164**

1) $g,h,x \in G$: $\pi_g \circ \pi_h(x) = \pi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \pi_{gh}(x) \Rightarrow \pi_g \circ \pi_h = \pi_{gh}$

$\phi(gh) = \pi_{gh} = \pi_g \circ \pi_h = \phi(g) \circ \phi(h) \Rightarrow$ ϕ ist Homomorphismus, um zu sehen, dass $\pi_g \in \mathrm{Aut}(G)$ siehe (2)

2) $\pi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \pi_g(x)\pi_g(y)$

$\pi_{g^{-1}}(\pi_g(x)) = \pi_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}g = x = gg^{-1}xgg^{-1} = \pi_g(\pi_{g^{-1}}(x)) \Rightarrow \pi_{g^{-1}} = (\pi_g)^{-1}$

Also ist $\pi_g \in \mathrm{Aut}(G)$

3) •) $\phi(g) = e \Leftrightarrow \pi_g = \mathrm{id} \Leftrightarrow \forall h \in G : \pi_g(h) = \ldots \Leftrightarrow \forall h \in G : ghg^{-1} = x \Leftrightarrow \forall h \in G : gh = hg$

$\Rightarrow \ker(\phi) = \{g \in G \mid \forall h \in G : gh = hg\}$

•) Sei $\phi : G \to \mathrm{Aut}(G)$ isomorphe Einbettung

Sei $g \in \ker\phi \Leftrightarrow \phi(g) = \pi_g = \mathrm{id} = \pi_g \circ (\pi_g)^{-1} = \pi_g \circ \pi_{g^{-1}} = \pi_{gg^{-1}} = \pi_e = \phi(e) \Leftrightarrow g = e \Rightarrow \ker\phi = \{e\}$

•) Sei $\ker\phi = \{e\}$ und $\phi(g) = \phi(h)$

$\pi_g = \pi_h \Leftrightarrow \pi_g \circ (\pi_h)^{-1} = \mathrm{id} \Leftrightarrow \pi_{gh^{-1}} = \mathrm{id} \Leftrightarrow \phi(gh^{-1}) = \mathrm{id} \Rightarrow gh^{-1} \in \ker\phi \Rightarrow gh^{-1} = e \Leftrightarrow g = h$

also ist Φ injektiv

4) Als Bild einer Untergruppe unter einem Homomorphismus ist $\phi(G)$ eine Untergruppe von $\mathrm{Aut}(G)$ (vgl. Prop. 2.3.1.24)

$f \in \mathrm{Aut}\,G$ bel. $\pi_g \in \phi(G)$, $h \in G$

$f(\pi_g(h)) = f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = \pi_{f(g)}(f(h)) \Rightarrow f \circ \pi_g = \pi_{f(g)} \circ f$

$\Rightarrow f \circ \phi(G) \subseteq \phi(G) \circ f \Rightarrow \phi(G) \lhd \mathrm{Aut}\,G$

UE 168 ► Übungsaufgabe 3.2.5.15. (F) Sei $G := S_4$. Wir geben die Elemente von G in Zyklenschreibweise an. Sei U die vom Element (1234) erzeugte Untergruppe und $N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Begründen Sie, warum $N \lhd S_4$ ein Normalteiler ist. Bestimmen Sie die Gruppen NU, $N \cap U$, NU/N, $U/(N \cap U)$ und geben Sie den kanonischen Isomorphismus zwischen NU/N und $U/(N \cap U)$ explizit an. **◄ UE 168**

N enthält vom Permutationstyp $(4, 0, \dots)$ ein Element und vom Permutationstyp $(0, 2, 0, \dots)$ (zählen der Länge 2) alle 3 Elemente und sonst keine, ist also nach Prop. 3.2.5.11 Punkt 4 ein Normalteiler von S_4

„U":

$(1234) \circ (1234) = (13)(24)$ und $(13)(24) \circ (1234) = (1234) \circ (13)(24) = (1432)$ (nach Prop. 3.2.5.19, weil alle Zyklen elementfremd sind)

$(1234) \circ (1432) = \mathrm{id}$ und $(1432) \circ (1234) = \mathrm{id}$ und $(1432) \circ (13)(24) = (13)(24) \circ (1432) = (1234)$

$(13)(24) \circ (13)(24) = \mathrm{id}$ und $(1432) \circ (1432) = (13)(24)$

wir erhalten $U = \langle 1234 \rangle = \{\mathrm{id}, (1234), (1432), (13)(24)\}$

„NU": $(12)(34) \circ (1234) = (1)(24)(3)$ und $(12)(34) \circ (1432) = (13)(2)(4)$ und $(12)(34) \circ (13)(24) = (14)(23)$ und

Da U Untergruppe von S_4 ist und $(13)(24) \in U$ gilt $(13)(24) \circ U = U$

$(14)(23) \circ (1234) = (13)(2)(4)$ und $(14)(23) \circ (1432) = (1)(24)(3)$ und $(14)(23) \circ (13)(24) = (12)(34)$

$NU = \{\mathrm{id}, (1234), (1432), (13)(24), (12)(34), (1)(24)(3), (13)(2)(4), (14)(23)\}$

„$N \cap U$": $N \cap U = \{\mathrm{id}, (13)(24)\}$ zur Kontrolle: ist wieder Untergruppe

„NU/N": $NU/N = \{\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}, \{(1234), (1432), (1)(24)(3), (13)(2)(4)\}\}$

„$U/N \cap U$": $U/N \cap U = \{\{\mathrm{id}, (13)(24)\}, \{(1432), (1234)\}\}$ Satz 3.2.1.4

$\varphi : NU/N \to U/N \cap U$:
$$\begin{cases} \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \longmapsto \{\mathrm{id}, (13)(24)\} \\ \{(1234), (1432), (1)(24)(3), (13)(2)(4)\} \longmapsto \{(1432), (1234)\} \end{cases}$$

Proposition 3.3.1.6. *Sei R ein Ring und $A \subseteq R$. Bezeichne I den Schnitt aller Ideale, $J \lhd R$ mit $A \subseteq J$. (I ist also das kleinste A umfassende Ideal in R, genannt das von A* erzeugte Ideal, *symbolisch $I = (A)$, im Fall $A = \{a_1, \ldots, a_n\}$ auch $I = (a_1, \ldots, a_n)$. Dann gilt:*

(1) *I ist die Menge aller*

$$\sum_{i=1}^{n} r_i a_i s_i + \sum_{j=1}^{m'} r'_j b_j + \sum_{k=1}^{n'} c_k s'_k + \sum_{l=1}^{m} d_l$$

mit $n, m', n', k \in \mathbb{N}$, $a_i, b_j, c_k, d_l \in A \cup -A$ und $r_i, s_i, r'_j, s'_k \in R$.

(2) *Hat R ein Einselement, so ist I auch darstellbar als die Menge aller*

$$\sum_{i=1}^{n} r_i a_i s_i$$

mit $n \in \mathbb{N}$, $a_i \in A$ und $r_i, s_i \in R$.

(3) *Ist R kommutativ mit 1, so ist (A) darstellbar als die Menge aller Summen (Linearkombinationen)*

$$\sum_{i=1}^{n} r_i a_i$$

mit $n \in \mathbb{N}$, $a_i \in A$ und $r_i \in R$. Ist außerdem $A = \{a\}$, einelementig, so ist

$$I = (a) = \{ra : \ r \in R\}.$$

UE 171 ► Übungsaufgabe 3.3.1.7. (V) Beweisen Sie Proposition 3.3.1.6. **◄ UE 171**

1) Wir zeigen, dass die angegebene Menge ein Ideal ist.

•) $0 + 0 = \left(\sum_{i=1}^{n} r_i a_i s_i + \sum_{j=1}^{n'} r_j' b_j + \sum_{k=1}^{n'} c_j s_j' + \sum_{l=1}^{m} d_l\right) + \left(\sum_{i=n+1}^{n+\tilde{n}} r_i a_i s_i + \sum_{j=n'+1}^{n'+n''} r_j' b_j + \sum_{k=n'+1}^{n'+n''} c_j s_j' + \sum_{l=m+1}^{m+\tilde{m}} d_l\right) =$

$$= \sum_{i=1}^{n'+n''} r_i a_i s_i + \sum_{j=1}^{m'+m''} r_j' b_j + \sum_{k=1}^{n'+n''} c_j s_j' + \sum_{l=1}^{m+\tilde{m}} d_l$$

•) $0 = \sum_{k \in \emptyset} a_k$

•) $-0 = -\left(\sum_{i=1}^{n} r_i a_i s_i + \sum_{j=1}^{n'} r_j' b_j + \sum_{k=1}^{n'} c_j s_j' + \sum_{l=1}^{m} d_l\right) = -\sum_{i=1}^{n} r_i a_i s_i - \sum_{j=1}^{n'} r_j' b_j - \sum_{k=1}^{n'} c_j s_j' - \sum_{l=1}^{m} d_l$ (wegen $d_l \in A \cup -A$)

Also handelt es sich um eine Untergruppe.

$r \in R$, dann ist $r\left(\sum_{i=1}^{n} r_i a_i s_i + \sum_{j=1}^{n'} r_j' b_j + \sum_{k=1}^{n'} c_j s_j' + \sum_{l=1}^{m} d_l\right) = \left(\sum_{i=1}^{n} r r_i a_i s_i + \sum_{k=1}^{n'} r c_j s_j'\right) + \left(\sum_{j=1}^{m'} r r_j' b_j + \sum_{l=1}^{m} r d_l\right)$

wieder in der Menge, also $rI \subseteq I$ und analog $Ir \subseteq I$ also ist die Menge ein Ideal.

2) $\sum_{l=1}^{m} d_l = \sum_{l=1}^{m} 1 d_l 1$ und $\sum_{k=1}^{n'} c_j s_j' = \sum_{k=1}^{n'} 1 c_j s_j' 1$ und $\sum_{j=1}^{m'} r_j' b_j = \sum_{j=1}^{m'} r_j' b_j 1$

3) $\sum_{i=1}^{n} r_i a_i s_i = \sum_{i=1}^{n} (r_i s_i) a_i$

Falls $A = \{a\}$: $\sum_{i=1}^{n} r_i a = \left(\sum_{i=1}^{n} r_i\right) a$

UE 172 ▶ Übungsaufgabe 3.3.1.10. (B) Geben Sie ein Beispiel eines Rings und eines Linksideals I an, sodass I kein Ideal ist. (Hinweis: Matrizen.) **◀ UE 172**

$R := \{A \in \mathbb{R}^{2\times 2}\}$ ein Ring mit 1, der nicht kommutativ ist.

$I := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$

I ist additive Untergruppe

$$\begin{pmatrix} u & x \\ v & y \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} au+bx & 0 \\ av+by & 0 \end{pmatrix} \in I \Rightarrow rI \subseteq I$$ also Linksideal, aber

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{\in I}\underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{\in R} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin I,$$ also kein Ideal.

Proposition 3.3.5.10. *1. Sei R ein Unterring mit 1 eines Körpers K. Dann ist*

$$K' := \{\frac{p}{q} : \ p, q \in R, q \neq 0\}$$

ein Unterkörper von K.

2. Der Körper K' aus dem ersten Teil ist der kleinste Unterkörper von K, der R enthält, symbolisch $K' = \langle R \rangle_{\text{Körper}}$. Explizit bedeutet das: Jeder Unterkörper K'' von K mit $R \subseteq K''$ umfasst K'.

3. In derselben Situation ist K (zusammen mit der Inklusionsabbildung) genau dann ein Quotientenkörper von R, wenn $K = K'$ gilt.

4. Ist $\iota\colon R \to K$ eine isomorphe Einbettung des Integritätsbereichs R in einen Körper K und Q der von $\iota(R)$ erzeugte Unterkörper von K, so ist Q zusammen mit ι ein Quotientenkörper von R.

UE 183 ▶ Übungsaufgabe 3.3.5.11. (W) Beweisen Sie 3.3.5.10. **◀ UE 183**

1) •) „+" $\frac{p}{q} + \frac{m}{n} = \frac{pn+mq}{qn} \in K'$, wobei $qn \neq 0$, weil $q, n \in K$ und K Körper $q, n \neq 0 \wedge$ Körper Nullteilerfrei

•) „0" $\frac{0}{1} \in K'$ neutrales Element bzgl. +

•) „1" $\frac{1}{1} \in K'$ neutrales Element bzgl. ·

•) „−" $\frac{p}{q} + \frac{-p}{q} = 0$

•) „$^{-1}$" $p \neq 0$ $\frac{p}{q} \cdot \frac{q}{p} = 1$

•) „·" $\frac{p}{q} \cdot \frac{m}{n} = \frac{pm}{qn} \in K'$

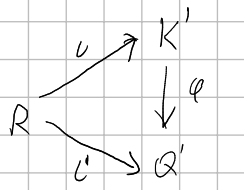
2) R ist sogar Integritätsbereich, weil der Körper K kommutativ ist und $0 \neq 1$ im Körper gilt

$R \setminus \{0\}$ ist ein kürzbares multiplikatives Untermonoid von R, denn $\frac{p}{q} \frac{m}{n} = \frac{p}{q} \frac{k}{e} \Rightarrow \frac{m}{n} = \frac{k}{e}$

Nach Satz 3.3.5.8 liegt mit K' ein Quotientenkörper von

Für einen beel. Körper Q', in welchen sich R isomorph

einbetten lässt, gibt es schon eine isomorphe Einbettung $\varphi\colon K' \to Q'$



Quotientenkörper sind bis auf Isomorphie eindeutig

3) „⇒" K Quotientenkörper von R, dann gilt nach Folgerung 3.3.5.3 $K \cong K'$

und wegen $K' \subseteq K \Rightarrow K' = K$

„⇐" K' ist Quotientenkörper und wegen $K' = K$ auch K

4) $\iota(R)$ ist Unterring mit 1 von Q, weil isomorphes Bild eines Integritätsbereiches. Nach (1) und (2) kennen wir Q', den kleinsten Unterkörper der $\iota(R)$ enthält. Aus (3) wissen wir, dass Q wegen $Q' = Q$ ein Quotientenkörper von $\iota(R)$ ist und da $\iota(R) \cong R$ ist Q auch Quotientenkörper zu R