F20T1A3 (V) (Abschluss)

ges: drei nicht abelsche, paarweise nicht isomorphe Gruppen der Ordnung $2002 = 2 \cdot 7 \cdot 11 \cdot 13$

Seien $N = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ und

$\iota_1, \iota_2 \in \mathrm{Aut}(N)$ geg. durch

$\iota_1(a,b,c) = (-a,b,c)$, $\iota_2(a,b,c) = (a,-b,c)$,

$\phi_1, \phi_2 : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(N)$ mit $\phi_1(\bar{0}) =$

$\phi_2(\bar{0}) = \mathrm{id}_N$, $\phi_1(\bar{1}) = \iota_1$, $\phi_2(\bar{1}) = \iota_2$

Seien $G_1 = D_{1001}$, $G_2 = N \rtimes_{\phi_1} \mathbb{Z}/2\mathbb{Z}$, $G_3 = N \rtimes_{\phi_2} \mathbb{Z}/2\mathbb{Z}$

Ziel: Zeige, dass G_1, G_2, G_3 paarweise nicht isomorph sind, weil sie unterschiedlich viele Elemente der Ordnung 2 besitzen.

bereits bekannt: $G_1 = D_{1001}$ hat genau 1001 Elemente der Ordnung 2.

Bestimmung der Anzahl in G_2: Sei $(a,b,c) \in N$.

Es gilt: $\operatorname{ord}((a,b,c),\bar{0}) \in \{1,2\} \iff$

$((a,b,c),\bar{0}) * ((a,b,c),\bar{0}) = e_{G_2} \iff$

$((a,b,c) + \phi_1(\bar{0})(a,b,c), \bar{0}+\bar{0}) = ((\bar{0},\bar{0},\bar{0}),\bar{0}) \iff$

$((a,b,c) + id_N(a,b,c), \bar{0}) = ((\bar{0},\bar{0},\bar{0}),\bar{0}) \iff$

$(a,b,c) + (a,b,c) = (\bar{0},\bar{0},\bar{0}) \iff$

$(2a, 2b, 2c) = (\bar{0}, \bar{0}, \bar{0}) \iff 2a = \bar{0} \wedge 2b = \bar{0} \wedge$
in $\mathbb{Z}/7\mathbb{Z}$ in $\mathbb{Z}/11\mathbb{Z}$
$2c = \bar{0} \overset{7,11,13}{\iff}$ $(a, b, c) = (\bar{0}, \bar{0}, \bar{0})$
in $\mathbb{Z}/13\mathbb{Z}$ ungerade

ebenso: $ord(((a,b,c), \bar{1})) \in \{1, 2\} \iff$

$((a,b,c), \bar{1}) * ((a,b,c), \bar{1}) = e_{G_2} \iff$

$((a,b,c) + \phi_1(\bar{1})(a,b,c), \bar{1} + \bar{1}) = ((\bar{0}, \bar{0}, \bar{0}), \bar{0}) \iff$

$((a,b,c) + \phi_1(a,b,c), \bar{0}) = ((\bar{0}, \bar{0}, \bar{0}), \bar{0}) \iff$

$(a,b,c) + (-a,b,c) = (\bar{0}, \bar{0}, \bar{0}) \iff$

$(0, 2b, 2c) = (\bar{0}, \bar{0}, \bar{0}) \iff 2b = \bar{0}, 2c = \bar{0}$

$\iff b = \bar{0}, c = \bar{0} \iff ((a,b,c), \bar{1}) \in$

$\{((a,\bar{0},\bar{0}),\bar{1}) \mid a \in \mathbb{Z}/7\mathbb{Z}\}$ (7 Elemente)

Insgesamt besitzt G_1 also $1+7=8$ Elemente der Ordnung 1 oder 2, also 7 Elemente der Ordn. 2.

Genauso zeigt man, dass G_2 genau 11 Elemente der Ordnung 2 besitzt. □

Aufgaben zu semidirekten Produkten:

F13T3A1 (konkretes Zahlenbsp)

H16T2A2 (Theorieaufg / Zahlenbsp)

F16T1A3*

Ringtheorie

Def. Ring = Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass gilt

(i) $(R, +)$ ist abelsche Gruppe
(Neutralelement = Nullelt. 0_R)

(ii) $(R, \cdot)$ ist abelsches Monoid
(Neutralelement = Einselt. 1_R)

(iii) Distributivgesetz: $\forall a, b, c \in R$:
$a \cdot (b + c) = a \cdot b + a \cdot c$

(In manchen Lehrbüchern wird bei (ii) nur gefordert, dass $(R, \cdot)$ eine Halbgruppe ist. Ist $\cdot$ kommutativ, dann

Def
(i)
(ii)
(iii)
(iv) Is
R
(In jede
Gruppe.

wird von einem kommutativen Ring gesprochen. Im Fall, dass $(R, \cdot)$ ein Monoid ist, heißt die Struktur Ring mit 1.)

Beispiele i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Ringe (aber nicht $\mathbb{N}, \mathbb{N}_0$)

ii) Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ (sind Körper genau dann, wenn n eine Primzahl ist)

iii) Über jedem Ring R kann der Polynomring $R[x]$ gebildet werden.

iv) Sind R und S Ringe, dann ist das direkte Produkt $R \times S$ ein Ring.

v) Ist R ein Ring und I ein Ideal, dann kann der Faktorring R/I gebildet werden.

Def.: Sei R ein Ring.

i) Ein Element $r \in R$ heißt Nullteiler, wenn ein $s \in R \setminus \{0_R\}$ mit $rs = 0_R$ existiert.

ii) Ein Element $r \in R$ heißt Einheit, wenn ein $s \in R$ mit $rs = 1_R$ existiert.
(Erinnerung: r Einheit $\Rightarrow$ r kein Nullteiler)

iii) Ist 0_R in R das einzige Nullteiler, dann nennt man R einen Integritätsbereich.

iv) Ist die Menge $R^\times$ der Einheiten gleich $R \setminus \{0_R\}$, dann heißt R Körper.

(In jedem Fall bilden die Einheiten eine Gruppe, die sog Einheitengruppe $R^\times$ des Rings.

Bsp.: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q}\setminus\{0\}$, $(\mathbb{Z}/n\mathbb{Z})^\times = \{a+n\mathbb{Z} \mid \mathrm{ggT}(a,n)=1\}$ Ist R ein Integritätsbereich, dann gilt $(R[x])^\times = R^\times$.)

F24T2A4 Entscheiden Sie (mit Begr.)

(a) Gibt es einen Rng R mit unendlich vielen Einheiten mit endlicher multiplikativer Ordnung?

Ja. Die Einheiten von $\mathbb{C}$ sind die Elemente von $\mathbb{C}\setminus\{0\}$. Die Menge $\{e^{2\pi i/n} \mid n\in\mathbb{N}\}$ ist unendlich, und jedes Element in dieser Menge hat eine endliche mult. Ordnung, da jeweils $(e^{2\pi i/n})^n = e^{(2\pi i/n)\cdot n} = e^{2\pi i} = 1$ gilt.

(b) Gibt es einen Rng mit unendlich vielen Einheiten endlicher additiver Ordnung?

Ja. Sei p eine beliebige Primzahl und $R = \mathbb{F}_p(x)$, der rationale Funktionenkörper über $\mathbb{F}_p$, d.h. der Quotientenkörper des Polynomrings $\mathbb{F}_p[x]$. Dieser ist unendlich, da bereits $\mathbb{F}_p[x]$ unendlich ist und $\mathbb{F}_p[x] \subseteq \mathbb{F}_p(x)$. Da $\mathbb{F}_p(x)$ ein Körper ist, gilt $\mathbb{F}_p(x)^\times = \mathbb{F}_p(x) \setminus \{\bar{0}\}$, und auch diese Menge ist somit unendlich. Da $\mathbb{F}_p(x)$ ein Körper der Charakteristik p ist, gilt für alle $u \in \mathbb{F}_p(x)^\times$ sowieso $pu = \bar{0}$, d.h. jedes solche Ele-

der Charakteristik p ist, gilt für alle $u \in F_{p^n}(x)^*$ zwar $pu = \bar{0}$, d.h. jedes solche Element hat eine endliche additive Ordnung.

(c) Gibt es einen Ring R mit nur endlich vielen Einheiten und eine Einheit unendlicher multiplikativer Ordnung?

Nein. Denn ang., R wäre ein solcher Ring. Auf Grund der Voraussetzung ist die Einheitengruppe $R^\times$ eine Gruppe mit endlicher Ordnung $n \in \mathbb{N}$. Für jedes $u \in R^\times$ gilt dann $u^n = 1_R$, d.h. jedes Element in $R^\times$ hat endliche Ordnung, und es gibt keine Elemente unendlicher Ordnung in $R^\times$. □

Übung: Gibt es einen Ring R mit endlich vielen Einheiten und eine Einheit unendlicher additiver Ordnung?

Def. Sei R ein Integritätsbereich. Ein Element $p \in R$ heißt (i) irreduzibel, wenn $r \neq 0_R$, $r \notin R^\times$ gilt und für alle $a, b \in R$ aus $r = ab$ jeweils $a \in R^\times$ oder $b \in R^\times$ folgt;

(ii) prim, wenn $r \neq 0_R$, $r \notin R^\times$ gilt und für alle $a, b \in R$ aus $p \mid (ab)$ jeweils $p \mid a$ oder $p \mid b$ folgt.

(Jedes Primelement in einem Integr.-bereich R ist irreduzibel.

$a, b \in R$ aus $p \mid (ab)$ jeweils $p \mid a$ oder $p \mid b$ folgt

(Jedes Primelement in einem Integ.-bereich R ist irreduzibel.

Die Umkehrung ist im Allg. falsch. Gegenbsp.:
$2 \in \mathbb{Z}[\sqrt{-3}]$ ist irreduzibel, aber kein Primelement.
denn: 2 ist Teiler von $4 = (1+\sqrt{-3})(1-\sqrt{-3})$, aber $2 \nmid (1 \pm \sqrt{-3})$.)

Bsp. Die irreduziblen Elemente, und zugleich die Primelemente, in $\mathbb{Z}$ sind gegeben durch $\pm p$, wobei p die Primzahlen durchläuft.

H24T1A3

Sei K ein Körper und

$$R = \left\{ \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_0, \dots, a_n \in K, a_1 = 0_K \right\}$$

(a) Zeigen Sie, dass R ein Teilring von $K[x]$ ist.

zu überprüfen: (1) $1_{K[x]} \in R$

(2) $\forall f, g \in R: f - g \in R$ und $fg \in R$

zu (1) Es gilt $1_{K[x]} = 1_K = a_1 x^1 + a_0 x^0$ mit $a_1 = 0_K$ und $a_0 = 1_K$. $\Rightarrow 1_{K[x]} \in R$

zu (2) Seien $f, g \in R$. $\Rightarrow \exists m, n \in \mathbb{N}$, $a_0, \dots, a_m \in R$, $b_0, \dots, b_n \in R$ mit

$f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{j=0}^{n} b_j x^j$, $a_1 = b_1 = 0_K$

Setze $r = \max\{m, n\}$, $a_i = 0_K$ für $m+1 \le i \le r$
$b_j = 0_K$ für $n+1 \le j \le r$. Dann gilt

$$f = \sum_{i=0}^{r} a_i x^i, \quad g = \sum_{i=0}^{r} b_i x^i \longrightarrow$$

$$f - g = \sum_{i=0}^{r} (a_i - b_i) x^i \text{ und } a_1 - b_1 = 0_K - 0_K = 0_K$$

$\Rightarrow f - g \in R$

Es gilt $f \cdot g = \sum_{k=0}^{m+n} c_k x^k$ mit $c_k = \sum_{i=0}^{k} a_{k-i} b_i$

und $c_1 = a_1 b_0 + a_0 b_1 = 0_K \cdot b_0 + a_0 \cdot 0_K = 0_K$

$\Rightarrow f \cdot g \in R$

(b) Untersuchen Sie, ob das Element x^3 in R irreduzibel bzw. prim ist.

Übung: F13T3A3, H16T1A3