Übungsblatt 4 - Jovan Petrov - Übungsgruppe 2 (Kohlhaum)

Aufgabe 2:

1. Wann ist $\sim_I$ $\quad a \sim_I b :\Leftrightarrow a = b + m$ für ein $m \in I, a, b \in R \supseteq I$ Äquivalenzrelation?

$\sim_I$ ist genau dann ÄR, wenn sie die folgenden Eigenschaften erfüllt:

- Reflexivität: $a \sim_I a \Leftrightarrow a = a + m$ für ein $m \in I$ g.d. erfüllt wenn $0_R \in I$, also g.d. wenn das neutrale Element bez. $+$ aus R in I ist.
- Symmetrie: $((a \sim_I b) \Rightarrow (b \sim_I a)) \Leftrightarrow (a = b + m_1, m_1 \in I) \Rightarrow (b = a + m_2, m_2 \in I)$ g.d. erfüllt wenn $\forall m \in I: (-m) \in I$, also g.d. wenn für jedes Element $m \in I \subseteq R$ das add. Inverse $(-m)$ aus R in I ist.
- Transitivität: $((a \sim_I b) \wedge (b \sim_I c)) \Rightarrow (a \sim_I c)) \Leftrightarrow$

$((a = b + m_1, m_1 \in I) \wedge (b = c + m_2 \in I) \Rightarrow (a = c + m_3 = c + m_1 + m_2, m_3 = m_1 + m_2 \in I))$

also g.d. erfüllt, wenn $m_1, m_2 \in I \Rightarrow m_1 + m_2 \in I$.

Dann ist also g.d. $\sim_I$ eine ÄR, wenn die folgenden Eigenschaften erfüllt sind:

1. $0_R \in I$
2. $m \in I \Rightarrow (-m) \in I$, $\quad m, (-m) \in R$
3. $m_1, m_2 \in I \Rightarrow m_1 + m_2 \in I$

2. $R/I := R/\sim_I$, wann sind $+, \cdot : R/I \times R/I \to R/I$ mit $[a] + [b] := [a +_R b]$, $[a] \cdot [b] := [a \cdot_R b]$ wohldefiniert?

* Addition: Seien $a_0 \in [a], b_0 \in [b]$ bel., d.h. $a_0 = a + m_1$, $b_0 = b + m_2$, $m_1, m_2 \in I$ für $a_0 + b_0 = a + m_1 + b + m_2 = (a+b) + (m_1 + m_2) = (a+b) + m_3$, $m_3 = m_1 + m_2 \in I$ nach Eigenschaft (3) aus 1. $\Rightarrow [a_0 + b_0] = [a+b]$. Für die Wohldefiniertheit der Addition genügen die 3 Eigenschaften aus 1.

* Multiplikation: Seien $a_0 \in [a]$, $b_0 \in [b]$ bel., $a, b \in R$ bel. d.h. $a_0 = a + m_1$, $b_0 = b + m_2 \in I$,

$$a_0 b_0 = (a+m_1)(b+m_2) = ab + am_2 + bm_1 + m_1 m_2$$

Damit $[a_0 b_0] = [ab]$ gilt, muss also

$ab + am_2 + bm_1 + m_1 m_2 = ab + m_3 \Leftrightarrow m_3 = am_2 + bm_1 + m_1 m_2 \in I$ gelten

Für $a = b = 0_R$ gilt $m_3 = m_1 m_2 \in I$. Also muss (*) $m_1, m_2 \in I \Rightarrow m_1 m_2 \in I$ erfüllt werden. D.h. also, dass $\cdot$ g.d. wohldefiniert ist, wenn für bel. $a, b \in R$ und m_1 aus m_2 $am_2 + bm_1 = \overset{I}{\overset{\in}{m_3}} + \overset{I}{\overset{\in}{(-m_1 m_2)}} \in I$.

Wir betrachten $b = 0_R \in R$. $\Rightarrow \forall a \in R, m \in I: am \in I$ gelten. Also ist diese Eigenschaft notwendig für die Wohldefiniertheit von $\cdot$. Diese ist auch hinreichend, da für bel. $a, b \in R$, $m_1, m_2 \in I$ $am_2, bm_1 \in I$ und damit auch $am_2 + bm_1 \in I$. Dann ist also die Multiplikation in R/I g.d. wohldefiniert wenn dazu noch

4. $\forall a \in R, m \in I: am \in I$ ((*) ist in 4. enthalten)

erfüllt ist.

3. R/I - Ring, wann ist er nullteilerfrei?

Damit R/I Integritätsbereich ist, muss $\forall a, b \in R$

$[ab] = [a][b] = [0] \Leftrightarrow [a] = [0] \vee [b] = [0]$ gelten. d.h.

Da $\forall c \in R: [c] = 0 \Leftrightarrow c = m \in I$ gilt ist R/I Integritäts bereich g.d. wenn noch zusätzlich:

5. $\forall a, b \in R: (ab \in I \Leftrightarrow a \in I \vee b \in I)$ ("$\Leftarrow$" ist in 4 enthalten)

erfüllt ist.

Aufgabe 3

1. $\frac{x^{p^2}-1}{x-1}$ - nicht irreduzibel

$$\frac{x^{p^2}-1}{x-1} = \frac{(x^p)^p - 1^p}{x-1} = \frac{(x^p-1)\left(\sum_{k=0}^{p-1} x^{kp}\right)}{(x-1)} = \left(\sum_{k=0}^{p-1} x^k\right)\left(\sum_{k=0}^{p-1} x^{kp}\right)$$

$$:= m(x)\,q(x) \quad , \; m(x), q(x) \in \mathbb{Z}[x]$$

$\text{Grad}(m(x)) = p-1$, $\text{Grad}(q(x)) = p(p-1) \Rightarrow \frac{x^{p^2}-1}{x-1}$ ist reduzibel.

2. Es gilt:

$$q(\zeta_{p^2}) = \sum_{k=0}^{p-1} \zeta_{p^2}^{kp} = \sum_{k=0}^{p-1} \left(e^{i\frac{2\pi}{p^2}}\right)^{kp} = \sum_{k=0}^{p-1} e^{\left(i\frac{2\pi}{p}\right)k} = \sum_{k=0}^{p-1} \zeta_p^k$$

$$\overset{\zeta_p \neq 1}{=} \frac{\zeta_p^p - 1}{\zeta_p - 1} = \frac{e^{i\frac{2\pi}{p}\cdot p} - 1}{\zeta_p - 1} = 0$$

Daher teilt das minpol$_{\zeta_{p^2}}$ $q(x)$. Wir beweisen, dass $q(x) = \text{minpol}_{\zeta_{p^2}}(x)$ gilt.

Sei $q'(y) = q(y+1) = \frac{(y+1)^{p^2}-1}{(y+1)^p - 1} \in \mathbb{Z}[x]$.

$$q'(y) = \frac{(y+1)^{p^2}-1}{(y+1)^p-1} = \frac{(y^p+1)^p - 1}{y^p + 1^p - 1} = \frac{y^{p^2} + 1^p - 1}{y + 1 - 1} = \frac{y^{p^2}}{y^p} = y^{p^2-p} \in \mathbb{F}_p[x]$$

$\text{grad}(q'(y)) = \text{grad}(q(x)) = p^2 - p$. Daher sind also alle Koeffizienten von $q'(y)$ in $\mathbb{Z}[y]$ außer dem leitenden Koeffizient durch p teilbar. Wir zeigen, dass p^2 nicht den Koeffizient a_0 von $q'(y) = a_{p^2-p}\, y^{p^2-p} + \ldots + a_0$ teilt.

$$q'(y) = q(y+1) = \sum_{k=0}^{p-1} (y+1)^{kp} = \sum_{k=0}^{p-1} \left(1 + \binom{kp}{1} y + \ldots + \binom{kp}{kp} y^{kp}\right)$$

$$= \sum_{k=0}^{p-1} 1 + \sum_{k=0}^{p-1}\sum_{j=1}^{kp} \binom{kp}{j} y^j = p + \sum_{k=0}^{p-1}\sum_{j=1}^{kp} \binom{kp}{j} y^j$$

da alle Summanden in $\sum_{k=0}^{p-1}\sum_{j=1}^{kp}\binom{kp}{j} y^j$ einen Faktor $y^j, j \neq 0$ haben gilt $p^2 \nmid p = a_0$. Daher ist $q'(y)$ und damit $q(x)$ nach dem Eisensteinkriterium irreduzibel und folglich gilt $q = \text{minpol}_{\zeta_{p^2}} =: \Phi_{p^2}$.

3. $$\Phi_{p^2}(\zeta_{p^2}^k) = \sum_{j=0}^{p-1} (\zeta_{p^2}^k)^{jp} = \sum_{j=0}^{p-1} \zeta_{p^2}^{kpj} = \sum_{j=0}^{p-1} e^{i\frac{2\pi}{p^2}kpj}$$
$$= \sum_{j=0}^{p-1} e^{i\frac{2\pi}{p}kj} = \sum_{j=0}^{p-1} (\zeta_p^k)^j = \frac{(\zeta_p^k)^p - 1}{\zeta_p^k - 1}, \quad \zeta_p^k \neq 1 \Leftrightarrow p \nmid k$$

Also gilt $\forall k \in \{0, \dots, p^2-1\}: p \nmid k: \Phi_{p^2}(\zeta_{p^2}^k) = 0$.

Für $p \mid k$ gilt $\Phi_{p^2}(\zeta_{p^2}^k) = \sum_{j=0}^{p-1} (\zeta_p^k)^j = \sum_{j=0}^{p-1} 1 = p \neq 0$. Es gilt also:

$\forall k \in \{0, \dots, p^2-1\}: \left(\Phi_{p^2}(\zeta_{p^2}^k) = 0 \Leftrightarrow p \nmid k\right)$.