Aufgabe F19T1A1 (12 Punkte)

(a) Bestimmen Sie das (multiplikative) Inverse von $\overline{47}$ im Restklassenring $\mathbb{Z}/112\mathbb{Z}$.

(b) Bestimmen Sie eine Zerlegung des Polynoms $2x^4 + 4x^3 + 4x^2 + 2x \in \mathbb{Z}[x]$ in irreduzible Faktoren aus $\mathbb{Z}[x]$.

(c) Geben Sie drei nichtisomorphe Gruppen der Ordnung 12 an (mit Begründung).

(d) Zeigen Sie, dass jede Gruppe der Ordnung 95 zyklisch ist.

Lösung:

zu (a) Wir wenden den euklidischen Algorithmus zur Bestimmung von $\mathrm{ggT}(112, 47)$ an.

q	a_n	x	y
–	112	1	0
–	47	0	1
2	18	1	-2
2	11	-2	5
1	7	3	-7
1	4	-5	12
1	3	8	-19
1	1	-13	31

An der letzten Tabellenzeile kann die Gleichung $1 = (-13)\cdot 112 + 31 \cdot 47$ abgelesen werden. Wegen $\overline{112} = \bar{0}$ in $\mathbb{Z}/112\mathbb{Z}$ folgt $(-\overline{13}) \cdot \bar{0} + \overline{31} \cdot \overline{47} = \bar{1}$, also $\overline{31} \cdot \overline{47} = \bar{1}$. Dies zeigt, dass $\overline{31}$ das multiplikative Inverse von $\overline{47}$ im Restklassenring $\mathbb{Z}/112\mathbb{Z}$ ist.

zu (b) Es gilt $2x^4+4x^3+4x^2+2x = 2x(x^3+2x^2+2x+1)$. Die Zahl -1 ist Nullstelle von x^3+2x^2+2x+1, und Polynomidivision liefert die Zerlegung $x^3 + 2x^2 + 2x + 1 = (x + 1)(x^2 + x + 1)$. Das Polynom $x + 1$ ist als Polynom vom Grad 1 irreduzibel in $\mathbb{Q}[x]$, außerdem als normiertes Polynom primitiv und somit ingesamt irreduzibel in $\mathbb{Z}[x]$. Aus denselben Gründen ist auch x in $\mathbb{Z}[x]$ irreduzibel. Als drittes Kreisteilungspolynom ist x^2+x+1 ebenfalls irreduzibel in $\mathbb{Z}[x]$. Schließlich ist 2 als Primzahl irreduzibel in $\mathbb{Z}$. Damit ist 2 auch in $\mathbb{Z}[x]$ irreduzibel. Denn weil $\mathbb{Z}$ ein Integritätsbereich ist, gilt $(\mathbb{Z}[x])^\times = \mathbb{Z}^\times = \{\pm 1\}$, also ist 2 in $\mathbb{Z}[x]$ keine Einheit. Gilt nun $2 = fg$ mit $f, g \in \mathbb{Z}[x]$, dann sind f und g Polynome vom Grad 0 und somit Elemente von $\mathbb{Z}$, und aus der Irreduziblität von 2 in $\mathbb{Z}$ folgt $f \in \{\pm 1\}$ oder $g \in \{\pm 1\}$, d.h. einer der beiden Faktoren ist eine Einheit in $\mathbb{Z}[x]$. Insgesamt ist $2 \cdot x \cdot (x + 1) \cdot (x^2 + x + 1)$ also eine Zerlegung des Polynoms in irreduzible Faktoren.

zu (c) Bekanntlich sind $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ und A_4 alles Gruppen der Ordnung 12. Die Gruppe A_4 ist nicht abelsch (denn beispielsweise gilt $(1\ 2\ 3) \circ (1\ 2\ 4) = (1\ 3)(2\ 4)$, aber $(1\ 2\ 4) \circ (1\ 2\ 3) = (1\ 4)(2\ 3) \neq (1\ 3)(2\ 4)$), während $\mathbb{Z}/12\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ abelsch sind. Somit ist A_4 weder zu $\mathbb{Z}/12\mathbb{Z}$ noch zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ isomorph. Die Gruppe $\mathbb{Z}/12\mathbb{Z}$ ist zyklisch, denn $\bar{1}$ ist wegen $n \cdot \bar{1} = \bar{n} \neq \bar{0}$ für $1 \leq n \leq 11$ und $12 \cdot \bar{1} = \overline{12} = \bar{0}$ ein Element der Ordnung 12. Dagegen ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ nicht zyklisch. Denn für alle $(\bar{a}, \bar{b}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ gilt $6(\bar{a}, \bar{b}) = (\overline{6a}, \overline{6b}) = (\bar{0}, \bar{0})$, somit ist die Ordnung jedes Elements in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ein Teiler von 6; insbesondere gilt es keine Elemente der Ordnung 12 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Dies zeigt, dass auch $\mathbb{Z}/12\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ nicht isomorph zueinander sind.

zu (d) Sei G eine Gruppe der Ordnung $95 = 5 \cdot 19$. Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Auf Grund des dritten Sylowsatzes gilt $\nu_{19} \mid 5$, also $\nu_{19} \in \{1, 5\}$, und außerdem $\nu_{19} \equiv 1 \bmod 19$. Wegen $5 \not\equiv 1 \bmod 19$ folgt daraus $\nu_{19} = 1$. Ebenso gilt $\nu_5 \mid 19$, also $\nu_5 \in \{1, 19\}$, und $\nu_5 \equiv 1 \bmod 5$. Wegen $19 \equiv 4 \not\equiv 1 \bmod 5$ folgt $\nu_5 = 1$. Sei P die einzige 5- und Q die einzige 19-Sylowgruppe von G. Wegen $\nu_5 = 1$ und $\nu_{19} = 1$ handelt es sich (nach dem 2. Sylowsatz) um Normalteiler von G.

Nun zeigen wir, dass G ein inneres direktes Produkt von P und Q ist. Dass $P \trianglelefteq G$ und $Q \trianglelefteq G$ gilt, haben wir bereits festgestellt. Weil $|P| = 5$ und $|Q| = 19$ teilerfremd sind, gilt $P \cap Q = \{e\}$. Sei nun $U = PQ$, das Komplexprodukt von P und Q. Wegen $P \trianglelefteq G$ handelt es sich um eine Untergruppe von G. Wegen $P \leq U$ und $Q \leq U$ ist $|U|$ nach dem Satz von Lagrange sowohl ein Vielfaches von $|P| = 5$ als auch ein Vielfaches von $|Q| = 19$, insgesamt also ein Vielfaches von $\mathrm{kgV}(5, 19) = 95$. Insbesondere gilt also $|U| \geq 95 = |G|$. Zusammen mit $U \subseteq G$ folgt daraus $G = U = PQ$.

Insgesamt ist damit nachgewiesen, dass G ein inneres direktes Produkt von P und Q ist. Es folgt $G \cong P \times Q$. Weil $|P| = 5$ und $|Q| = 19$ Primzahlen sind, handelt es sich bei P und Q um zyklische Gruppen. Daraus folgt $P \cong \mathbb{Z}/5\mathbb{Z}$ und $Q \cong \mathbb{Z}/19\mathbb{Z}$, also $G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$. Wegen $\mathrm{ggT}(5, 19) = 1$ kann der Chinesische Restsatz angewendet werden und liefert $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \cong \mathbb{Z}/95\mathbb{Z}$. Aus $G \cong \mathbb{Z}/95\mathbb{Z}$ folgt schließlich, dass auch G eine zyklische Gruppe ist.