Lösung zur Klausur zur Vorlesung „Diskrete Strukturen“

Marc Ensenbach

19. Juli 2001

Ankreuzteil

Aufgabe A1
(1) Ja. Dies wurde in der Vorlesung gezeigt.
(2) Nein. Die Stirlingzahlen 1. Art geben die Anzahl der Permutationen in der symmetrischen Gruppe S_n an, die aus k ziffernfremden Zyklen bestehen. Summiert man alle $s_{n,k}$ für festes n auf, so erhält man $|S_n| = n!$. Da $1! \neq 2^1$ ist, gilt die Behauptung nicht.
(3) 7. Berechnung mit Hilfe der Rekursionsformel aus (1): $S_{4,2} = S_{3,1} + 2S_{3,2} = 1 + 2 \cdot 3 = 7$.

Aufgabe A2
(1) Nein. Sei $A = 1 + x$, dann ist $A^2 = 1 + 2x + x^2 \neq 1 + x = 1^2 + 1^2x$.
(2) Ja. $x^2A = x^2 \sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{\infty} a_k x^{k+2} = \sum_{n=2}^{\infty} a_{n-2} x^n$ mit Indexverschiebung $n = k + 2$.
(3) Nein. $A = 2$ ist eine formale Potenzreihe (mit einem Glied) mit $A^{-1} = \frac{1}{2}$ in $\mathbb{Q}$.

Aufgabe A3
(1) Nein. Über $K = \mathbb{Z}_2$ ist $(x^2 + x + 1)^2 = x^4 + x^2 + 1 =: f$, also ist dieses Polynom nicht irreduzibel. Würde $(x + c)|f$ für ein $c \in K$ gelten, so wäre $-c$ eine Nullstelle des Polynoms. Es gilt aber hier $f(0) = 1 = f(1)$, also teilt weder x noch $x + 1$ das Polynom. Die Folgerung kann daher im allgemeinen nicht gelten.
(2) Ja. Satz der Vorlesung.
(3) Ja. Siehe Übungaufgabe 27.

Aufgabe A4
(1) 9. $\mathbb{Z}/9\mathbb{Z} = \{0 + 9\mathbb{Z}; 1 + 9\mathbb{Z}; 2 + 9\mathbb{Z}; \ldots; 8 + 9\mathbb{Z}\}$.
(2) Nein. In $\mathbb{Z}/9\mathbb{Z}$ ist $3 \cdot 3 = 9 = 0$, also ist $\mathbb{Z}/9\mathbb{Z}$ nicht nullteilerfrei und damit kein Körper.
(3) 9. Sei $f \in \mathbb{Z}_3[x]$. Dann existieren Polynome $q, r \in \mathbb{Z}_3[x]$ mit $f = q(x^2 - 1) + r$ und $\operatorname{Grad} r < 2$ oder $r = 0$. Da $[f]_{x^2-1} = [q(x^2 - 1) + r]_{x^2-1} = [r]_{x^2-1}$ ist, bilden die Polynome in $\mathbb{Z}_3[x]$ mit einem Grad kleiner 2 ein Vertretersystem aller Elemente von $\mathbb{Z}_3[x]/(x^2 - 1)\mathbb{Z}_3[x]$; es gibt genau $3^2 = 9$ solcher Polynome.
(4) Nein. Da $x^2 - 1 = (x + 1)(x - 1)$ nicht irreduzibel ist, kann $\mathbb{Z}_3[X]/(x^2 - 1)\mathbb{Z}_3[X]$ nach A3(2) kein Körper sein.

Aufgabe A5
(1) 3. Vergleiche vorletzte Präsenzübung.
(2) Nein. Vergleiche vorletzte Präsenzübung.
(3) Nein. Vergleiche vorletzte Präsenzübung.

Aufgabe A6

(1) Nein. Nach dem Handschlag-Lemma ist $\sum_{v\in V} d(v)$ immer gerade.

(2) Nein. Ein Graph mit 5 Knoten kann höchstens $\binom{5}{2} = 10$ Kanten haben, daher muß $\sum_{v\in V} d(v) = 2|E| \leqslant 20$ gelten.

(3) Nein. Da die Hauptdiagonalelemente von A^2 gerade 1 sein sollen, muß gelten: $1 = (A^2)_{ii} = \sum_{j=1}^{3} a_{ij}a_{ji}$. Da A als Adjazenzmatrix symmetrisch ist, gilt $a_{ji} = a_{ij}$, also ist $(A^2)_{ii} = \sum_{j=1}^{3} a_{ij}^2$. Da die Adjazenzmatrix über $\mathbb{Z}$ aufgefaßt wird, muß genau eins der Quadrate a_{ij}^2 gleich 1 sein, damit die Bedingung erfüllt ist, also muß in jeder Zeile genau eine 1 vorkommen. Man versuche, eine Adjazenzmatrix, also eine symmetrische Matrix mit Nullen auf der Hauptdiagonalen zu konstruieren, die diese Eigenschaft erfüllt. Dies ist nicht möglich.

Rechenaufgaben ohne Begründung

Aufgabe R1

(1) 12. Nach Vorlesung ist $|\operatorname{Inj}(\{1;2\};\{1;2;3;4\})| = |\{1;2;3;4\}|^{\underline{|\{1;2\}|}} = 4^{\underline{2}} = 4\cdot 3 = 12$.

(2) 36. Vorlesung: $|\operatorname{Surj}(\{1;2;3;4\};\{1;2;3\})| = |\{1;2;3\}|!\cdot S_{|\{1;2;3;4\}|,|\{1;2;3\}|} = 3!S_{4,3} = 6\cdot 6 = 36$.

(3) 24. Da Definitions- und Zielmenge gleichmächtig sind, gilt $|\operatorname{Inj}(\{1;2;3;4\};\{1;2;3;4\})| = |\operatorname{Bij}(\{1;2;3;4\};\{1;2;3;4\})| = |\{1;2;3;4\}|! = 4! = 24$.

Aufgabe R2

(1) Die Zykeldarstellung ist klarerweise $(1\ 7\ 2\ 5)(4\ 8\ 6)$.

(2) 15. Die Ordnung ist das positive kgV der einzelnen Zykellängen, sofern die Zykeln ziffernfremd sind, hier also $15 \in \operatorname{kgV}(3;5)$.

(3) Die Darstellung lautet $(3\ 8\ 6\ 4\ 7)$.

(4) Die Darstellung ist $(1\ 2\ 5)(3\ 6\ 7\ 8\ 4)$, da $a^{3001} = a^{20\cdot 15+1} = \left(a^{15}\right)^{20} a = a$.

Aufgabe R3

$14 = 9\cdot 532 - 11\cdot 434$. Nach dem Euklidischen Algorithmus ist $532 = 1\cdot 434 + 98$, $434 = 4\cdot 98 + 42$, $98 = 2\cdot 42 + 14$, $42 = 3\cdot 14$, also ist 14 ein ggT von 532 und 434. Durch Rückwärtsauflösen erhält man $14 = 98 - 2\cdot 42 = (532 - 1\cdot 434) - 2\cdot(434 - 4\cdot 98) = 532 - 3\cdot 434 + 8\cdot 98 = 532 - 3\cdot 434 + 8\cdot(532 - 434) = 9\cdot 532 - 11\cdot 434$.

Aufgabe R4

(1) 16. $\varphi(60) = \varphi(2^2\cdot 3\cdot 5) = \varphi(2^2)\cdot\varphi(3)\cdot\varphi(5) = 2\cdot 2\cdot 4 = 16$.

(2) 16. Die Eulersche φ-Funktion gibt gerade die Anzahl der invertierbaren Elemente an.

(3) 49. Nach dem Satz von Euler ist $7^{162} = \left(7^{16}\right)^{10}\cdot 7^2 \equiv 7^2 = 49 \mod 60$, da $1 \in \operatorname{ggT}(7;60)$.

Aufgabe R5

(1) 8. Die irreduziblen Teiler von $x^{2^5} - x$ sind nach Vorlesung gerade die irreduziblen Polynome von einem Grad, der 5 teilt, also vom Grad 1 oder Grad 5. In Teil (2) werden wir sehen, daß es genau 6 irreduzible Polynome vom Grad 5 gibt; die irreduziblen Polynome vom Grad 1 sind gerade x und $x+1$, also gibt es insgesamt 8 irreduzible Teiler von $x^{2^5} - x$.

(2) 6. Nach Vorlesung ist die gesuchte Anzahl $N_5(2) = \frac{1}{5}\sum_{d|5}\mu(d)2^{\frac{5}{d}} = \frac{1}{5}(\mu(1)2^5 + \mu(5)2^1) = \frac{1}{5}(32-2) = 6$.

Aufgabe R6

4. Die Ideale eines Ringes $K[x]/fK[x]$ sind gerade die $gK[x]/fK[x]$ mit $g|f$, suche daher die normierten Teiler von x^5+1 in $\mathbb{Z}_2[x]$. Es gilt $x^5+1=(x+1)(x^4+x^3+x^2+x+1)$, wobei die Polynome auf der rechten Seite irreduzibel sind. Aus dieser Darstellung kann man die Teiler ablesen: 1, $x+1$, $x^4+x^3+x^2+x+1$ und x^5+1. Daher gibt es vier (normierte) Teiler und damit vier Ideale.

Aufgaben mit Lösungsweg

Aufgabe L1

Sei $A=\sum_{n=0}^{\infty} a_n x^n$. Dann gilt $A=a_0+a_1x+\sum_{n=2}^{\infty} a_n x^n$. Setzt man die Anfangsbedingungen und die Rekursionsformel ein, erhält man $A = 2x + \sum_{n=2}^{\infty}(-a_{n-1}+2a_{n-2})x^n = 2x - \sum_{n=2}^{\infty} a_{n-1}x^n + 2\sum_{n=2}^{\infty} a_{n-2}x^n = 2x - x\sum_{n=2}^{\infty} a_{n-1}x^{n-1} + 2x^2\sum_{n=2}^{\infty} a_{n-2}x^{n-2} \overset{a_0=0}{=} 2x - x\sum_{n=0}^{\infty} a_n x^n + 2x^2\sum_{n=0}^{\infty} a_n x^n = 2x - xA + 2x^2A$, durch Auflösen nach A folgt $A=\frac{2x}{1+x-2x^2}$. Das reflektierte Polynom des Nenners lautet x^2+x-2, es hat die Nullstellen $\beta=1$ und $\gamma=-2$. Damit läßt sich A darstellen als $\frac{2x}{(1-x)(1+2x)}$. Nun setzt man mit Partialbruchzerlegung an: $\frac{2x}{(1-x)(1+2x)} = \frac{B}{1-x}+\frac{C}{1+2x} \Leftrightarrow 2x=(1+2x)B+(1-x)C = B+2xB+C-xC = (B+C)+x(2B-C)$. Durch Koeffizientenvergleich erhält man $B+C=0 \wedge 2B-C=2 \quad\Leftrightarrow\quad C=-B \wedge 3B=2 \quad\Leftrightarrow\quad B=\frac{2}{3} \wedge C=-\frac{2}{3}$. Analog zum Beispiel der Fibonacci-Folge aus der Vorlesung erhält man $a_n = B\beta^n + C\gamma^n = \frac{2}{3}\cdot 1^n - \frac{2}{3}(-2)^n = \frac{2}{3}(1-(-2)^n)$.

Aufgabe L2

Nach dem chinesischen Restsatz ist $\psi : \mathbb{Z}_{220} \to \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{11}$, $[z]_{220} \mapsto ([z]_4;[z]_5;[z]_{11})$ ein möglicher Isomorphismus. Damit hat man $\psi([135]_{220}) = ([135]_4;[135]_5;[135]_{11}) = ([3]_4;[0]_5;[3]_{11})$ und $\psi([187]_{220}) = ([187]_4;[187]_5;[187]_{11}) = ([3]_4;[2]_5;[0]_{11})$. Da ψ ein Isomorphismus ist, darf man komponentenweise multiplizieren. Damit erhält man $\psi([135\cdot 187]_{220}) = ([3]_4[3]_4;[0]_5[2]_5;[3]_{11}[0]_{11}) = ([9]_4;[0]_5;[0]_{11}) = ([1]_4;[0]_5;[0]_{11})$. Um das Ergebnis von $[135]_{220}\cdot[187]_{220}$ in $\mathbb{Z}_{220}$ zu erhalten, muß man folgende (simultane) Kongruenzen lösen: $z\equiv 1 \mod 4$, $z\equiv 0 \mod 5$, $z \equiv 0 \mod 11$. Die letzten beiden Bedingungen bedeuten, daß z durch 55 teilbar sein muß. Es bietet sich daher an, die kleinen Vielfachen von 55 auf ihre Reste mod 4 zu untersuchen: $55\equiv 3 \mod 4$, $110\equiv 2 \mod 4$, $165\equiv 1 \mod 4$, also erfüllt 165 alle Kongruenzen simultan. Damit ist $[135]_{220}\cdot[187]_{220} = [165]_{220}$ in $\mathbb{Z}_{220}$.