Relaties en Structuren: oefeningen

Eerste Bachelor Wiskunde

Jan De Beule – Bert Seghers

29 januari 2013, 8:30

1. Zij R en $\overline{R}$ twee relaties op een verzameling A. Definieer

$$R_0 = R \text{ en } R_i = R_{i-1} \cup \{(x,z) \in A \times A \mid \exists y \in A : x\ R_{i-1}\ y \wedge y\ R_{i-1}\ z\}.$$

Bewijs nu dat de volgende uitspraken equivalent zijn.

- $\overline{R} = \bigcup_{i=0}^{\infty} R_i$.
- $\overline{R}$ is transitief *en* $R \subseteq \overline{R}$ *en* voor elke relatie S die transitief is en waarvoor $R \subseteq S$, geldt dat $\overline{R} \subseteq S$.

Oplossing. Stel eerst $\overline{R} = \bigcup_{i=0}^{\infty} R_i$. Duidelijk is $R = R_0 \subseteq \bigcup_{i=0}^{\infty} R_i = \overline{R}$.

Bovendien is $\bigcup_{i=0}^{\infty} R_i$ transitief, want neem $(a,b) \in \bigcup_{i=0}^{\infty} R_i$ en $(b,c) \in \bigcup_{i=0}^{\infty} R_i$. Dan bestaan er een j en een k zodat $(a,b) \in R_j$ en $(b,c) \in R_k$. Omdat $R_m \subseteq R_n$ als $m < n$, zijn (a,b) en (b,c) dus beiden bevat in $R_{\max(j,k)}$. Per definitie van $R_{\max(j,k)+1}$ is het koppel (a,c) dan bevat in $R_{\max(j,k)+1}$ en dus zeker in $\bigcup_{i=0}^{\infty} R_i$. Dat bewijst de transitiviteit.

Neem nu een relatie S die transitief is met de eigenschap dat $R \subseteq S$. We moeten bewijzen dat $\bigcup_{i=0}^{\infty} R_i \subseteq S$. Daarvoor zal het volstaan om te bewijzen: $\forall i \in \mathbb{N} : R_i \subseteq S$. Dit bewijzen we met inductie op i. Voor $i = 0$ is het triviaal, want de onderstelling op S zegt dat $R_0 = R \subseteq S$. Stel nu als inductiehypothese dat $R_{i-1} \subseteq S$. Neem $(x,y) \in R_i$; we willen bewijzen dat $(x,y) \in S$. Er zijn twee mogelijkheden (per definitie van R_i): ofwel zit (x,y) al in R_{i-1}, ofwel bestaat er een z zodat (x,z) en (z,y) in R_{i-1} zitten. In het eerste geval is meteen $(x,y) \in S$ door de inductiehypothese. In het tweede geval zijn (x,z) en (z,y) eveneens bevat in S wegens de inductiehypothese en wegens de transitiviteit van S dan ook (x,y).

Stel omgekeerd dat $\overline{R}$ een relatie is waarvoor de drie eigenschappen gelden uit de tweede uitspraak. We moeten twee inclusies bewijzen. Om te bewijzen dat $\bigcup_{i=0}^{\infty} R_i \subseteq \overline{R}$, zullen we wederom $\forall i \in \mathbb{N} : R_i \subseteq \overline{R}$ bewijzen. Dit is compleet analoog aan de voorgaande paragraaf (inductie op i, vervang S door $\overline{R}$).

Om te bewijzen dat $\overline{R} \subseteq \bigcup_{i=0}^{\infty} R_i$, volstaat het om het gegeven "Voor elke relatie S die transitief is en waarvoor $R \subseteq S$, geldt dat $\overline{R} \subseteq S$" te instantiëren voor $S = \bigcup_{i=0}^{\infty} R_i$. Inderdaad, we hebben in het begin bewezen dat $\bigcup_{i=0}^{\infty} R_i$ een transitieve relatie is die R omvat. Het gegeven zegt ons dan dat $\overline{R} \subseteq \bigcup_{i=0}^{\infty} R_i$.

2. Aan het oefeningenexamen Relaties en Structuren, dat uit vijf vragen bestaat, doen 36 studenten mee. Veronderstel dat de antwoorden binair verbeterd worden als *juist* of *fout*. Als je weet dat elke vraag door minstens de helft van de studenten juist werd beantwoord, bewijs dan dat er twee studenten zijn waarvoor elke vraag door minstens één van die twee succesvol is opgelost.

Oplossing. Uit een dubbele telling van de koppels {(student,vraag) | student heeft vraag juist} blijkt dat het gemiddeld aantal juist beantwoorde vragen per student ten minste 2.5 is. Dat

betekent dat er zeker een student is die (minstens) drie vragen juist heeft. Laten we hem Klaas noemen en veronderstel zonder verlies van algemeenheid dat hij vragen 1, 2 en 3 correct beantwoordde. Als Klaas vier of vijf vragen juist heeft, dan is het meteen bewezen: neem één van die minstens 18 studenten die de (eventuele) vraag juist had die Klaas fout had, dan hebben ze samen alles juist. We kunnen dus onderstellen dat Klaas *enkel* vragen 1, 2 en 3 juist had. Van de 35 andere studenten (niet Klaas) zijn er minstens 18 die vraag 4 juist hadden, en ook minstens 18 die vraag 5 juist hadden. Maar omdat $35 < 18+18$, moeten deze verzamelingen een niet-ledige doorsnede hebben. Een student uit die doorsnede heeft dan vragen 5 *en* 6 correct, en heeft samen met Klaas alle vragen correct.

3. (a) Bepaal de laatste twee cijfers van

$$20\,142\,013^{\left(554\,433^{2018}\right)}.$$

(b) Zijn p en q verschillende oneven priemgetallen. Bewijs dat, als -1 een kwadraat is modulo pq, dan

$$p+q \equiv pq+1 \pmod{16}.$$

Is het omgekeerde ook waar?

(c) Los op:

$$x^2 \equiv -1 \pmod{130}$$

Oplossing.

(a) Omdat $\varphi(100) = 40$, is $20\,142\,013^{40} \equiv 1 \pmod{100}$, dus het volstaat om de exponent modulo 40 te bepalen. Omdat $\varphi(40) = 16$, is $554\,433^{16} \equiv 1 \pmod{40}$, dus het volstaat om de exponent modulo 16 te bepalen. Daar $2018 \equiv 2 \pmod{16}$, is $554\,433^{2018} \equiv 554\,433^2 \equiv 33^2 \equiv (-7)^2 \equiv 49 \equiv 9 \pmod{40}$. Zo wordt

$$20\,142\,013^{\left(554\,433^{2018}\right)} \equiv 20\,142\,013^9 \equiv 13^9 \equiv (13^3)^3 \equiv (-3)^3 \equiv -27 \equiv 73 \pmod{100}.$$

(b) Als -1 een kwadraat is modulo pq, dan is $x^2 \equiv -1 \pmod{pq}$ een oplosbare vergelijking, die wegens de Chinese reststelling equivalent is met het stelsel

$$\begin{cases} x^2 \equiv -1 \pmod{p} \\ x^2 \equiv -1 \pmod{q}, \end{cases}$$

dat dus ook oplossingen moet hebben. Dat betekent echter dat -1 een kwadraat is modulo p, en ook een kwadraat modulo q. Maar -1 is een kwadraat modulo p als en slechts als $p \equiv 1 \pmod{4}$, dus we vinden dat $4 \mid p-1$ en dat $4 \mid q-1$. Dan is $16 \mid (p-1)(q-1) = pq-p-q+1$, of, anders gezegd, $p+q \equiv pq+1 \pmod{16}$.

Het omgekeerde is niet waar. De implicatie $4 \mid p-1 \wedge 4 \mid q-1 \Rightarrow 16 \mid (p-1)(q-1)$ is namelijk niet omkeerbaar. Als bijvoorbeeld $p-1 = 16$ en $q-1 = 2$, dan is het consequens wel waar maar het antedent niet. Inderdaad, modulo $17 \cdot 3$ is -1 geen kwadraat.

(c) Via het algoritme van de Chinese reststelling is dit te herleiden tot

$$\begin{cases} x \equiv -1 \pmod{2} \\ x \equiv \pm 2 \pmod{5} \\ x \equiv \pm 5 \pmod{13} \end{cases}$$

en men vindt de oplossingen 47, 57, 73 en 83 modulo 130.

4. Bewijs dat

$$\sum_{k=0}^{n} \binom{n}{k} S(k,d) \;=\; S(n+1,d+1)$$

Oplossing. Zij N een verzameling met n elementen. Het linkerlid telt het aantal mogelijkheden om een *deelverzameling* van N (van orde $k \in \{0,\ldots,n\}$) te partitioneren in d nietledige klassen. Er zijn namelijk $\binom{n}{k}$ mogelijkheden om die deelverzameling van orde k te kiezen en voor elk ervan zijn er $S(k,d)$ mogelijkheden om die k elementen in d nietledige klassen te partitioneren (als $k < d$, is $S(k,d) = 0$). Voeg nu een nieuw element ♠ toe aan N, zodat $|N \cup \spadesuit| = n+1$. Het rechterlid telt alle mogelijke partities van $N \cup \{\spadesuit\}$ in $d+1$ klassen.

We leggen nu een bijectie tussen beide soorten partities. We vertrekken van een partitie van een *deelverzameling* K van N in d klassen (dus van het soort dat in het linkerlid werd geteld) en construeren een partitie van $N \cup \{\spadesuit\}$ in $d+1$ klassen (dus van het soort dat in het rechterlid geteld werd). De bijectie: voeg één extra klasse toe, bestaande uit het element ♠ en alle elementen van $N \setminus K$. Dit zal inderdaad een partitie opleveren van $N \cup \{\spadesuit\}$, waarvan alle klassen nietledig zijn. De inverse bijectie is ook gemakkelijk te construeren: verwijder uit $N \cup \{\spadesuit\}$ het element ♠ en verwijder uit de partitie het element dat ♠ bevat.

5. (a) Construeer het eindig veld $\mathbb{F}_{32}$ met het irreducibele polynoom

$$f(x) = x^5 + x^2 + 1 \quad \in \mathbb{F}_2[x]$$

en stel de Zech-log-tabel op.

(b) Los over deze $\mathbb{F}_{32}$ de vergelijking $X^2 + (\alpha^4 + \alpha^2)X + 1 = 0$ op, indien mogelijk.

(c) Bewijs dat elk irreducibel polynoom van graad 5 over $\mathbb{F}_2$ primitief is.

(d) Bewijs dat $\mathbb{F}_{32}$ geen deelvelden heeft buiten $\mathbb{F}_2$ en $\mathbb{F}_{32}$ zelf.

Oplossing.

(a) We berekenen opeenvolgende machten van α, waarbij $\alpha^5 = \alpha^2 + 1$, om de Zech-log-tabel op te stellen.

$a^\infty = 0$	$a^{10} = a^4 + 1$	$a^{21} = a^4 + a^3$
$a^0 = 1$	$a^{11} = a^2 + a + 1$	$a^{22} = a^4 + a^2 + 1$
$a^1 = a$	$a^{12} = a^3 + a^2 + a$	$a^{23} = a^3 + a^2 + a + 1$
$a^2 = a^2$	$a^{13} = a^4 + a^3 + a^2$	$a^{24} = a^4 + a^3 + a^2 + a$
$a^3 = a^3$	$a^{14} = a^4 + a^3 + a^2 + 1$	$a^{25} = a^4 + a^3 + 1$
$a^4 = a^4$	$a^{15} = a^4 + a^3 + a^2 + a + 1$	$a^{26} = a^4 + a^2 + a + 1$
$a^5 = a^2 + 1$	$a^{16} = a^4 + a^3 + a + 1$	$a^{27} = a^3 + a + 1$
$a^6 = a^3 + a$	$a^{17} = a^4 + a + 1$	$a^{28} = a^4 + a^2 + a$
$a^7 = a^4 + a^2$	$a^{18} = a + 1$	$a^{29} = a^3 + 1$
$a^8 = a^3 + a^2 + 1$	$a^{19} = a^2 + a$	$a^{30} = a^4 + a$
$a^9 = a^4 + a^3 + a$	$a^{20} = a^3 + a^2$	$(a^{31} = 1)$

We vinden de volgende Zech-log-tabel, waarvan we de helft geven (de andere helft is symmetrisch):

0	∞	4	10	9	16	15	24
1	18	6	27	11	19	17	30
2	5	7	22	12	23	21	25
3	29	8	20	13	14	26	28

(b) We vinden met de Zech-log-tabel dat $\alpha^2 + \alpha^4 = \alpha^7$. We delen de vergelijking door $(\alpha^7)^2$ en vinden de gereduceerde vergelijking $Y^2 + Y + \delta$, met $Y = X/\alpha^7$ en $\delta = \alpha^{-14} = \alpha^{17}$. Nu is

$$\begin{aligned}
\mathrm{Tr}(\delta) = \mathrm{Tr}(\alpha^{17}) &= \alpha^{17} + \left(\alpha^{17}\right)^2 + \left(\alpha^{17}\right)^4 + \left(\alpha^{17}\right)^8 + \left(\alpha^{17}\right)^{16} \\
&= \alpha^{17} + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{24} \\
&= \alpha^3(\alpha^{14} + 1) + \alpha^6(\alpha^6 + 1) + \alpha^{24} \\
&= \alpha^{16} + \alpha^2 + \alpha^{24} \\
&= \alpha^2(\alpha^{14} + 1) + \alpha^{24} \\
&= \alpha^{15} + \alpha^{24} \\
&= \alpha^{15}(\alpha^9 + 1) \\
&= \alpha^{15}\alpha^{16} = \alpha^{31} = 1
\end{aligned}$$

Daaruit blijkt dat de vergelijking geen oplossingen heeft.

(c) Neem een willekeurig irreducibel polynoom f van graad 5 over $\mathbb{F}_2$ en stel daarmee het eindig veld $\mathbb{F}_{32}$ op in α, met $f(\alpha) = 0$. De multiplicatieve groep van dit veld is een cyclische groep van orde 31, een priemgetal. Elk element van die cyclische groep, behalve 1, zal dus de hele groep voortbrengen. In het bijzonder is dat het geval voor de wortel α. Maar dat de wortel α van f de multiplicatieve groep van het eindig veld voortbrengt, is per definitie wat de betekenis is van "f is een primitief polynoom".

(d) Stel dat $K \subseteq \mathbb{F}_{32}$ een deelveld is. Dan is $\mathbb{F}_{32}$ een vectorruimte over dat deelveld K (de axioma's van een vectorruimte zijn voldaan). Bijgevolg is de orde van de vectorruimte $\mathbb{F}_{32}$ een macht van de orde van het scalairenveld K, dus $32 = |K|^n$. Echter, de enige mogelijkheden zijn hier $|K| = 2$ of $|K| = 32$.

Alternatief, als K een deelveld is, dan is zijn multiplicatieve groep $K \setminus \{0\}$ ook een deelgroep van de multiplicatieve groep van het grote veld $\mathbb{F}_{32}$, d.w.z.

$$K \setminus \{0\}, \cdot \leq \mathbb{F}_{32} \setminus \{0\}, \cdot.$$

Echter, wegens de stelling van Lagrange is de orde van deze deelgroep een deler van de orde van de groep, dus

$$|K| - 1 \;\mid\; 31$$

Dit kan enkel wanneer $|K| = 2$ (geeft aanleiding tot $K = \mathbb{F}_2 \leq \mathbb{F}_{32}$) of $|K| = 32$ (geeft aanleiding tot $K = \mathbb{F}_{32} \leq \mathbb{F}_{32}$)