

Lösningssförslag till uppgift 6 från övning 13

Uppgift

Låt $k = \{0, 1, a, 1 + a\}$ vara kroppen med fyra element.

- Skriv upp additions- och multiplikationstabellerna för k .
- Bestäm en matris med koefficienter i $\mathbb{Z}_2$ sådan att k kan representeras av matriserna $\{0, I, A, A + I\}$.

Lösningssförslag

- Vi börjar med att notera att $|k| = 2^2$, så att $\text{char}(k) = 2$, det vill säga att $2 = 0$ (och därmed $-1 = 1$) i k . Additionstabellen fås från detta direkt:

+	0	1	a	$1 + a$
0	0	1	a	$1 + a$
1	1	0	$1 + a$	a
a	a	$1 + a$	0	1
$1 + a$	$1 + a$	a	1	0

Vi börjar med att delvis fylla i multiplikationstabellen genom att använda att $0 \cdot x = 0$ och $1 \cdot x = x$ för alla $x \in k$:

$\cdot$	0	1	a	$1 + a$
0	0	0	0	0
1	0	1	a	$1 + a$
a	0	a		
$1 + a$	0	$1 + a$		

(1)

Vi måste nu bestämma a^2 . Notera att $a^2 \neq 0$, eftersom $a \neq 0$ och k är en kropp, och notera även att $a^2 \neq a$ (annars hade ekvationen kunnat divideras med a för att få $a = 1$). Vi måste alltså antingen ha $a^2 = 1$ eller $a^2 = 1 + a$.

Det kan inte gälla att $a^2 = 1$, för detta hade medfört att $(1 + a)^2 = 1^2 + a^2 = 1 + 1 = 0$, vilket inte kan gälla då $1 + a \neq 0$ och k är en kropp. Ett annat sätt att se att $a^2 \neq 1$ är att notera att om $a^2 = 1$, så är $a(1 + a) = a + 1 = 1 + a$, vilket ger $a = 1$. Ett tredje sätt är att se att $a^2 = 1$ hade inneburit att a är en rot till polynomet $x^2 - 1 = (x + 1)(x - 1) = (x - 1)^2$, som ger att $a = 1$.

När vi väl vet att $a^2 = 1 + a$ följer det sen att $(1 + a)a = a + 1 + a = 1 + 2a = 1$, och $(1 + a)^2 = 1 + 2a + a^2 = 1 + 0a + 1 + a = a$, och att $a(1 + a) = 1$ då produkten är kommutativ. Detta ger multiplikationstabellen

$\cdot$	0	1	a	$1 + a$
0	0	0	0	0
1	0	1	a	$1 + a$
a	0	a	$1 + a$	1
$1 + a$	0	$1 + a$	1	a

(2)

Notera att alla rader och kolonner i multiplikationstabellen, förutom den första raden och första kolonnen, innehåller alla fyra element i k . Detta gäller för en multiplikationstabell i alla ändliga kroppar, eftersom ekvationen $x \cdot y = x \cdot z$ kan divideras med x för att få $y = z$. Om vi utgår från tabellen (1) finns det bara ett sätt att fylla i den som uppfyller detta, nämligen som i (2). Detta är ett alternativt sätt att lösa uppgiften på, utan att resonera om a^2 .

- Vi vill att matriserna A och $A + I$ ska bete sig som elementen a och $1 + a$ vad gäller multiplikation. Det gäller automatiskt att $0 \cdot A = 0$ och $1 \cdot A = A$, oavsett vilken matris A vi väljer, och vi såg i resonemanget ovan att resterande produkter bestäms unikt från att $a^2 = 1 + a$. Vi behöver alltså hitta en matris A som uppfyller $A^2 = I + A$, eller ekvivalent, $A^2 - A - I = 0$. En matris med karakteristiskt polynom $p_A(x) = x^2 - x - 1 = 0$ kommer på grund av Cayley–Hamiltons sats att uppfylla detta. Ett allmänt sätt att få en matris med det karakteristiska (och även minimala) polynomet $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ är att ta matrisen

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix},$$

och i vårt fall är $n = 2$ och $a_0 = -1 = 1$ och $a_1 = -1 = 1$, så vi kan välja $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.