Esimerkki polynomien jaollisuudesta

Kerkko Luosto

26. marraskuuta 2014

Jaottomia polynomeja $(\mathbb{Z}/2\mathbb{Z}[x], +, \cdot)$:ssa

p	$p(0)$	$p(1)$	juurten joukko	jaottomuus
x				jaoton
$x+1$				jaoton
x^2				
x^2+1				
x^2+x				
x^2+x+1				
x^3				
x^3+1				
x^3+x				
x^3+x+1				
x^3+x^2				
x^3+x^2+1				
x^3+x^2+x				
x^3+x^2+x+1				

Jaottomia polynomeja $(\mathbb{Z}/2\mathbb{Z}[x], +, \cdot)$:ssa

p	$p(0)$	$p(1)$	juurten joukko	jaottomuus
x	0			jaoton
$x+1$	1			jaoton
x^2	0			
x^2+1	1			
x^2+x	0			
x^2+x+1	1			
x^3	0			
x^3+1	1			
x^3+x	0			
x^3+x+1	1			
x^3+x^2	0			
x^3+x^2+1	1			
x^3+x^2+x	0			
x^3+x^2+x+1	1			

Jaottomia polynomeja $(\mathbb{Z}/2\mathbb{Z}[x], +, \cdot)$:ssa

p	$p(0)$	$p(1)$	juurten joukko	jaottomuus
x	0	1		jaoton
$x+1$	1	0		jaoton
x^2	0	1		
x^2+1	1	0		
x^2+x	0	0		
x^2+x+1	1	1		
x^3	0	1		
x^3+1	1	0		
x^3+x	0	0		
x^3+x+1	1	1		
x^3+x^2	0	0		
x^3+x^2+1	1	1		
x^3+x^2+x	0	1		
x^3+x^2+x+1	1	0		

Jaottomia polynomeja $(\mathbb{Z}/2\mathbb{Z}[x], +, \cdot)$:ssa

p	$p(0)$	$p(1)$	juurten joukko	jaottomuus
x	0	1	$\{0\}$	jaoton
$x+1$	1	0	$\{1\}$	jaoton
x^2	0	1	$\{0\}$	
x^2+1	1	0	$\{1\}$	
x^2+x	0	0	$\{0,1\}$	
x^2+x+1	1	1	$\emptyset$	
x^3	0	1	$\{0\}$	
x^3+1	1	0	$\{1\}$	
x^3+x	0	0	$\{0,1\}$	
x^3+x+1	1	1	$\emptyset$	
x^3+x^2	0	0	$\{0,1\}$	
x^3+x^2+1	1	1	$\emptyset$	
x^3+x^2+x	0	1	$\{0\}$	
x^3+x^2+x+1	1	0	$\{1\}$	

Jaottomia polynomeja $(\mathbb{Z}/2\mathbb{Z}[x], +, \cdot)$:ssa

p	$p(0)$	$p(1)$	juurten joukko	jaottomuus
x	0	1	$\{0\}$	jaoton
$x+1$	1	0	$\{1\}$	jaoton
x^2	0	1	$\{0\}$	
x^2+1	1	0	$\{1\}$	
x^2+x	0	0	$\{0,1\}$	
x^2+x+1	1	1	$\emptyset$	jaoton
x^3	0	1	$\{0\}$	
x^3+1	1	0	$\{1\}$	
x^3+x	0	0	$\{0,1\}$	
x^3+x+1	1	1	$\emptyset$	jaoton
x^3+x^2	0	0	$\{0,1\}$	
x^3+x^2+1	1	1	$\emptyset$	jaoton
x^3+x^2+x	0	1	$\{0\}$	
x^3+x^2+x+1	1	0	$\{1\}$	

Jaottomasta polynomista kunnaksi

Kunnan $\mathbb{Z}_2 = (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ polynomirenkaan jaottomat polynomit, joiden aste on korkeintaan 3, ovat siis x, $x+1$, x^2+x+1, x^3+x+1 ja x^3+x^2+1.

Jaottomasta polynomista kunnaksi

Kunnan $\mathbb{Z}_2 = (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ polynomirenkaan jaottomat polynomit, joiden aste on korkeintaan 3, ovat siis x, $x+1$, x^2+x+1, x^3+x+1 ja x^3+x^2+1.

Jatketaan esimerkkiä tarkastelemalla erityisesti jaotonta polynomia x^3+x+1. Jaottomuudesta seuraa siis, että $\langle x^3+x+1\rangle$ on maksimaalinen ideaali ja $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ on kunta.

Jaottomasta polynomista kunnaksi

Kunnan $\mathbb{Z}_2 = (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ polynomirenkaan jaottomat polynomit, joiden aste on korkeintaan 3, ovat siis x, $x+1$, x^2+x+1, x^3+x+1 ja x^3+x^2+1.

Jatketaan esimerkkiä tarkastelemalla erityisesti jaotonta polynomia x^3+x+1. Jaottomuudesta seuraa siis, että $\langle x^3+x+1\rangle$ on maksimaalinen ideaali ja $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ on kunta. Jokaisella $p \in (\mathbb{Z}/2\mathbb{Z})[x]$ on jakoyhtälön nojalla olemassa sellaiset $q, r \in (\mathbb{Z}/2\mathbb{Z})[x]$, että

$$p = (x^3+x+1)\cdot q + r,$$

missä $\deg(r) < \deg(x^3+x+1) = 3$, jolloin

$$p + \langle x^3+x+1\rangle = r + \langle x^3+x+1\rangle.$$

Jaottomasta polynomista kunnaksi II

Koska polynomeja $r \in (\mathbb{Z}/2\mathbb{Z})[x]$, joille $\deg(r) \leq 2$, on $2^3 = 8$ kappaletta, niin kunnassa $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ on korkeintaan 8 alkiota.

Jaottomasta polynomista kunnaksi II

Koska polynomeja $r \in (\mathbb{Z}/2\mathbb{Z})[x]$, joille $\deg(r) \leq 2$, on $2^3 = 8$ kappaletta, niin kunnassa $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ on korkeintaan 8 alkiota. Toisaalta jakoyhtälön jaon yksikäsitteisyydestä seuraa, että $r + \langle x^3 + x + 1 \rangle \neq r' + \langle x^3 + x + 1 \rangle$, kun $r \neq r'$ ja $\deg(r) \leq 2$, $\deg(r') \leq 2$. Siis alkioita on täsmälleen 8.

Jaottomasta polynomista kunnaksi II

Koska polynomeja $r \in (\mathbb{Z}/2\mathbb{Z})[x]$, joille $\deg(r) \leq 2$, on $2^3 = 8$ kappaletta, niin kunnassa $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ on korkeintaan 8 alkiota. Toisaalta jakoyhtälön jaon yksikäsitteisyydestä seuraa, että $r + \langle x^3 + x + 1\rangle \neq r' + \langle x^3 + x + 1\rangle$, kun $r \neq r'$ ja $\deg(r) \leq 2$, $\deg(r') \leq 2$. Siis alkioita on täsmälleen 8.

Merkitään $I = \langle x^3 + x + 1\rangle$. Konkreettisissa laskuissa on käytännöllistä merkitä $p \equiv q \pmod{I}$, kun $p, q \in (\mathbb{Z}/2\mathbb{Z})[x]$. Yhteen- ja kertolaskutauluissa esiintyy alkioiden sijasta ekvivalenssiluokkien edustajia eli polynomeja.

Yhteenlaskutaulu

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0								
1								
x								
$x+1$								
x^2								
x^2+1								
x^2+x								
x^2+x+1								

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x						
$x+1$	0	$x+1$						
x^2	0	x^2						
x^2+1	0	x^2+1						
x^2+x	0	x^2+x						
x^2+x+1	0	x^2+x+1						

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x				
$x+1$	0	$x+1$	x^2+x	x^2+1				
x^2	0	x^2						
x^2+1	0	x^2+1						
x^2+x	0	x^2+x						
x^2+x+1	0	x^2+x+1						

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$			
$x+1$	0	$x+1$	x^2+x	x^2+1				
x^2	0	x^2	$x+1$					
x^2+1	0	x^2+1						
x^2+x	0	x^2+x						
x^2+x+1	0	x^2+x+1						

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1				
x^2	0	x^2	$x+1$					
x^2+1	0	x^2+1	1					
x^2+x	0	x^2+x	x^2+x+1					
x^2+x+1	0	x^2+x+1	x^2+1					

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1				
x^2+1	0	x^2+1	1	x^2				
x^2+x	0	x^2+x	x^2+x+1	1				
x^2+x+1	0	x^2+x+1	x^2+1	x				

Kertolaskutaulu

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$