Delgrupper av cykliska grupper.

Anmärkning

Varje delgrupp av en cyklisk grupp är cyklisk.

Exempel

Beskriva alla delgrupper av $\mathbb{Z}_6$.

Ringar.

Definition

En **ring** $(R, +, \cdot)$ är en mängd med två binära operationer sådan att:

1. $(R, +)$ är en kommutativ grupp.
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ för alla $a, b, c \in R$.
3. $a \cdot (b + c) = a \cdot b + b \cdot c$, för alla $a, b, c \in R$.
4. $(a + b) \cdot c = a \cdot c + b \cdot c$, för alla $a, b, c \in R$.

Exempel

1. $(\mathbb{Z}, +, \cdot), (\mathbb{R}, +\cdot)$ *är ringar.*
2. *för varje* $n \geq 2$ *är* $(\mathbb{Z}_2, +, \cdot)$ *en ring.*
3. $(M_2(\mathbb{R}), +, \cdot)$ *är en ring.*

Om $\cdot$ är kommutativ dåkllas ringen en **kommutativ ring.**

Definition

1. Ett element u i en ring $(R, +, \cdot)$ kallas en **etta** (multiplikativ identitet) om

$$a \cdot u = u \cdot a = a \text{ för alla } a \in R.$$

   En ring med ett sådant element kallar vi ring med etta.

2. Låt $(R, +, \cdot)$ vara en ring med etta. Ett elemnt $a \in R$ kallas **inverterbart** om det finns ett elemnt b (den multiplikativ invers) sådan att

$$a \cdot b = b \cdot a = u.$$

Inverterbara elementa

Låt R vara en ring med etta. Vi definierar:

$$U(R) = \{a \in R \text{ sådan att } a \text{ är inverterbart}\}.$$

Anmärkning

$(U(R), \cdot)$ är en grupp.

Exempel

$$U((\mathbb{Z}_n, \cdot)) = \{[m], (m, n) = 1.\}$$

Så $(U(\mathbb{Z}_n), \cdot)$ är en grupp med $\phi(n)$ många element.

$$U((\mathbb{Z}_6) = \{1, 5\} \cong \mathbb{Z}_2, U(\mathbb{Z}_5) = \{1, 2, 3, 4\}$$

Kroppar

Definition

En kommutativ ring med etta i vilken varje element utom noll är inverterbart kallas en **kropp**. En kropp är då en mängd med två operationer $(K, +, \cdot)$ där:

- $(K, +)$ är en kommutativ grupp,
- $(K - \{0\}, \cdot)$ är en kommutativ grupp.

Exempel

- $(\mathbb{Z}, +, \cdot)$ *är inte en kropp.* $(\mathbb{R}, +, \cdot)$
- $(\mathbb{Z}_p, +, \cdot)$ *där* p *är ett primtal är en kropp.*

Polynom över en kropp

Låt F vara en kropp. Vi betecknar nollan (den additiv identitet) med 0 och ettan med 1.
Ett formellt uttryck av formen:

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

där koefficienterna a_i tillhör kroppen F or x är en obestämd, kallas **polynom** över F av **grad** n.
Två polynom definieras som lika om de har samma koefficienterna.

Polynom över en kropp

Man kan definiera de (vanliga) additionen och multiplikationen av två polynom:

$$(x^3 + a_2x^2 + a_1x + a_0) + (b_2x^2 + b_1x + b_0) =$$

$$= x^3 + (a_2 + b_2)x^2 + (a_1 + b_1)x + (a_0 + b_0)$$

$$(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) =$$

$$= (a_2b_2)x^4 + (a_1b_2 + b_1a_2)x^3 + (a_1b_1 + a - 2b_0 + a_0b_2)x^2$$

$$+(a_1b_0 + a_0b_1)x + (a_0b_0)$$

Exempel

I $\mathbb{Z}_5$ *är*

$$(1 + 2x^2)(1 + 3x) = 1 + 3x + 2x^2 + x^3.$$

Notera att $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$.

delbarhet av polynom

Definition

Man säger att $g(x)$ delar $f(x)$ $(g(x)|f(x))$ om det finns ett polynom $k(x) \neq 1$ så dan att

$$f(x) = g(x)k(x).$$

Exempel

$$(x+1)|(x^2-1) \;\; i\, \mathbb{R}[x].$$

Ett polynom av grad minst två son saknar äkta delare kallas ett irreducibelt (oreducerbart) polynom.
$x^2 + 1$ är irreducibelt på $\mathbb{R}$.

delbarhet av polynom

SATS

Låt $f(x), g(x)$ vara polynom över en kropp K. Då fins entydigt bestämda polynom $q(x), r(x)$ så dan att:

$$f(x) = q(x)g(x) + r(x)$$

och $deg(r(x)) < deg(g(x))$.

Exempel

I $\mathbb{Z}_3$ är:

$$x^4 + x^2 + x + 1 = (x^2 + 2x + 2)(x^2 + x) + (2x + 1)$$

delbarhet av polynom

Definition

Låt $f(x)$ vara ett polynom med koefficienterna i en kropp F och $a \in F$. Om $f(a) = 0$ då kallas a ett nollställe av f.

Exempel

- *polynomet* $x^2 - 2$ *med koefficienterna i* $\mathbb{R}$ *har nollställena* $\pm\sqrt{2}$.
- *polynomet* $x^2 - 2$ *med koefficienterna i* $\mathbb{Z}_3$ *saknar nollställen.*

Anmärkning

Elementet $a \in F$ är ett nolställe till $f(x)$ om och endast om $(x - a)|f(x)$, d.v.s

$$f(x) = (x - a)g(x)\ deg(g(x)) = deg(f(x)) - 1.$$

Exempel

Exempel

Skriv $f(x) = x^4 + 1$ *som en produkt av irreducibla polynom på* $\mathbb{Z}_3$.

Eftersom $f(x)$ har inga nollställe ska alla faktorerna ha grad minst 2. Det enda möjlighet är två faktorer av grad två.

$$x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D)$$

ger $B = D = 2, A = 1, C = 2$.