MAT1100 - Grublegruppen
Notat 10

Jørgen O. Lye

Ringer

Vi fortsetter i et lynkurs i algebraiske dyr. Først ut er ringer. En ring A (også kalt R) er en abelsk gruppe med addisjon $+$ som operasjon. I tillegg skal man ha en multiplikasjon som ikke trenger å oppfylle gruppetingene. Derimot skal man kreve følgende for alle $x, y, z \in A$:

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $(x + y) \cdot z = x \cdot z + y \cdot z$

Så kommer det store spørsmålet: skal man kreve at det finnes et element $1 \in A$ som er slik at $x \cdot 1 = 1 \cdot x = x$ for alle x? Dette er en konvensjonssak. Kursene på Blindern er ikke helt enige. Det er ikke uvanlig å kreve $1 \in A$, men det er ikke nødvendig.

Merk et par ting som glimrer med sitt fravær. Det står ikke at $x \cdot y = y \cdot x$. Ringer hvor det holder kalles komutative ringer, og er de grunnleggende størrelsene i kommutativ algebra. Vanlige tall tilfredsstiller dette, matriser gjør det ikke. Hvis man krever $1 \in A$ så er det definitivt ikke vanlig å kreve at alle ting har en multiplikativ invers. Dvs man krever ikke at det finnes x^{-1} slik at $x \cdot x^{-1} = 1$. Dette betyr at A er en gruppe med hensyn på addisjon, men ikke med hensyn på multiplikasjon, selv om man tar med 1. Ihvertfall ikke generelt (det finnes selvsagt ringer som har multiplikative inverser).

Notasjonsmessig kommer vi fra nå av til å droppe $\cdot$ og bare skrive xy for $x \cdot y$.

Eksempler på ringer

En prototyp (komutativ) ring er $\mathbb{Z}$ med addisjon og multiplikasjon som man lærer på barneskolen. I $\mathbb{Z}$ finnes 1, men bare 1 og -1 har multiplikativ invers: $\frac{1}{x}$ er ikke i $\mathbb{Z}$ utenom de 2 unntakene.

En annen ring er

$$M_n(\mathbb{K}) = \{\text{Alle } n \times n \text{ matriser med koeffisienter i } \mathbb{K}\}$$

Merk at vi ikke heller her krever inverterbare matriser. I denne ringen er $1 = \mathbb{1}$. Denne ringen er ikke kommutativ, og er et godt eksempel på hvordan de kan se ut.

Litt mer eksotisk, men litt nærmere kalkulus, er

$$C^\infty(U) = \{f : U \to \mathbb{R} \big| f \text{ er uendelig ganger deriverbar}\}$$

hvor U er en (åpen) mengde i $\mathbb{R}^n$ for den n man vil. Dette er en kommutativ ring med 1, hvor 1 her betyr funksjonen fra U til $\mathbb{R}$ som er konstant 1. Dette er et eksempel på hvordan ringer kan oppstå utenfor algebra.

En ring som også er mer enn en ring (mer om dette snart) er $\mathbb{R}$ eller $\mathbb{C}$. Disse er kommutative ringer med 1, og her kan man invertere alt annet enn 0. Dvs $\frac{1}{x}$ finnes i $\mathbb{R}$ eller $\mathbb{C}$ når $x \neq 0$. $\mathbb{Q}$ hadde også fungert her.

En veldig viktig ring for algebraikere er polynomringer: $A = \mathbb{K}[x]$ ={Alle polynomer p(x) med koeffisienter i $\mathbb{K}$} Husk at per definisjon er ikke ting some $\frac{1}{x}$ et polynom, så man kan generelt sett ikke dele her heller. Hvis man vil ha polynomer i flere variable skriver man $\mathbb{K}[x_1, \cdots x_n]$.

Idealer

Et ideal $\mathfrak{a} \subset A$ fungerer litt som normale undergrupper. De er definert ved at man krever

- $\mathfrak{a}$ skal være en undergruppe med addisjon
- $ax \in \mathfrak{a}$ og $xa \in \mathfrak{a}$ for alle $x \in A$, alle $a \in \mathfrak{a}$

Punkt nummer 2 uttrykkes gjerne ved at $\mathfrak{a}$ skal være lukket under multplikasjon fra A. Merk at vi trengte å skrive ax og xa siden vi ikke har antatt at ringen er kommutativ.

La oss herfra anta at ringen er kommutativ, for å gjøre livet lettere. Dette er uansett veldig vanlig å se på dette tilfellet for seg. Et ideal $\mathfrak{p} \neq A$[1] kalles et primideal dersom $xy \in \mathfrak{p} \iff x \in \mathfrak{p}$ eller $y \in \mathfrak{p}$.

[1]Betingelsen $\mathfrak{a} \neq A$ er igjen en konvensjon. Den er praktisk, men det er ikke sikkert alle er enige.

Eksempler

En type ideal man alltid kan lage seg er $(a) = \{ax\, x \in A\}$ Dvs alle multipler av et eller annet element i ringen A. Eksempelet rett under burde klargjøre dette. Av og til skriver man $(a)A$ for å understreke hvilken ring man tenker på, men vi dropper det.

$A = \mathbb{Z}$

La $A = \mathbb{Z}$. Da er $(n) = \{x \big| x = na,\, a \in \mathbb{Z}\}$ med ord: (n) er alle multipler av n. F.eks er (2) alle partallene, (1) er hele ringen $\mathbb{Z}$, mens (3) $= \{\cdots, -6, -3, 0, 3, 6 \cdots\}$

Man kan vise at disse er idealer. Det er heller ikke så grusomt vanskelig å vise at (p) er et primideal hvis og bare hvis $p = 0$ eller p er et primtall. Så hvis man vi studere primtall så kan man studere ikke-null primidealer i $\mathbb{Z}$ heller. Dette er starten på en del algebraisk maskineri for å drive med tallteori.

$A = \mathbb{C}[z]$

Ringen er alle polynomer i en variabel med koeffisienter i $\mathbb{C}$. Som før kan man velge seg et polynom $p(z)$ og se på $(p(z))$. Dette er alle polynomer som inneholder $p(z)$ som en faktor. Geometrisk kan man tenke på $(p(z))$ som alle polynomer med nullpunktene til $p(z)$ (og kanskje flere nullpunkter). Spesielt vil (z) være alle polynomer som er 0 i 0, mens $(z - a)$ er alle polynomer som er 0 i a, $a \in \mathbb{C}$.

Hvis man husker at alle polynomer faktoriserer komplekst, dvs $p(z) = c(z - z_0)(z - z_1) \cdots (z - z_n)$, så klarer man kanskje å vise at ting på formen $(z - a)$ er primidealer i $\mathbb{C}[z]$.

Kvotientringer

I likhet med normale grupper så vil $A/\mathfrak{a}$ bli en ring hvor man regner "modulo $\mathfrak{a}$". Eksempler er kanskje veien å gå:

$$\mathbb{Z}/(n) = \mathbb{Z}_n$$

$$\mathbb{K}[x]/(x) = \mathbb{K}$$

Mer fancy er kanskje at

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C} \tag{1}$$

Her er det et par ord å si. Hvis A og B er ringer, så er $\phi : A \to B$ er en ring-homomorfi dersom $\phi(ab) = \phi(a)\phi(b)$ og $\phi(a + b) = \phi(a) + \phi(b)$. Hvis 1

er med, så skal $\phi(1) = 1$. En isomorfi er en interverterbar homomorfi hvor inversen også er en homomorfi. Dette er hva jeg mener med $\cong$.

Avbildningen i 1 er $\phi : \mathbb{R}[x] \to \mathbb{C}$, $x \mapsto i$. Denne er ikke injektiv, siden alle polynomer med $(x^2 + 1)$ med faktor sendes til 0 selv om disse polynomene ikke er 0 i $\mathbb{R}[x]$. Hvis man derimot tenker på alle slike polynomer som det samme, dvs regner modulo idealet generert av $x^2 + 1$, altså $(x^2 + 1)$, så er avbildningen injektiv! Den er ganske klart surjektiv fra før av, slik at på ringen $\mathbb{R}[x]/(x^2 + 1)$ er den injektiv og surjektiv.

Hvis dette eksempelet faller tungt, kan man bare ta det som fancy algebra man kan lære i kurset MAT2200, "Grupper, ringer og kropper".

Man kan tenke på eksempelet på følgende intuitive måte. Venstresiden sier at man har polynomer med relle koeffisienter: $p(x) = a_n x^n + \cdots a_0$. Når man deler ut med $(x^2 + 1)$, så kan man ennå skrive polynomet sitt som før, men alle x^2 kan/skal byttes ut med -1, siden $x^2 + 1$ og 0 er "det samme" i kvotientringen. Dette er presist hvordan dere fikk beskjed om å regne med komplekse tall tidlig i MAT1100: bare regn med i som en vanlig variabel, men bytt ut i^2 med -1.

Kropper

En kropp k er en kommutativ ring med 1 som oppfyller enda mer. For alle $x \neq 0$ i k skal det finnes $x^{-1} \in k$ slik at $xx^{-1} = 1$. Dette er på en måte den strengeste interessante konstruksjonen i algebra. Eksemplene er $\mathbb{R}$, $\mathbb{Q}$ og $\mathbb{C}$. Eksempler på ting som ikke er kropper er $\mathbb{K}[x]$ siden man ikke kan dele på x der, og $\mathbb{Z}$ siden man ikke kan dele på noe annet enn 1 og -1.

Kropper virker veldig praktiske å jobbe med, men de mangler dessverre en del interessant struktur ringer har. Følgende oppgave oppgave illustrerer dette, som man kan løse med å se på defisjonen av et ideal og definisjonen av en kropp: La k være en kropp, og anta $\mathfrak{a} \subset k$ er et ideal. Da er $\mathfrak{a} = k$ eller $\mathfrak{a} = \{0\}$. Det er de eneste mulighetene.

Spesielt vil man ikke ha skikkelige primidealer i en kropp. Så tallteori-oppsetttet man hadde tenkt å kjøre igang på primtallene krasjer hvis man bruker $\mathbb{R}$ eller $\mathbb{Q}$ istedenfor $\mathbb{Z}$. Dette visste man vel egentlig fra før av: alle primtall kan skrives som produkt av 2 andre tall i $\mathbb{R}$ og $\mathbb{Q}$ (på uendelig mange måter) og mister litt statusen sin som spesielle tall.

Det finnes flere annet ganske viktige eksempler på kropper, ihvertfall hvis man er algebraiker. Hvis p er et primtall, så påstår jeg at $\mathbb{Z}/(p)$ er en kropp. Egentlig påstår jeg litt mer: jeg påstår $\mathbb{Z}/(p)$ er en kropp hvis og bare hvis p er et primtall. Husk at ringen $\mathbb{Z}/(p)$ kan tenkes på som tallene $\{0, 1, \cdots p-1\}$ hvor både addisjon og multiplikajon skjer modulo p. Et eksempel er for $p = 3$.

Da er mengden $\{0, 1, 2\}$ og regnereglene er ting som $2 \cdot 1 = 2$, $2 \cdot 2 = 1$, $2 + 1 = 0$, $2 + 2 = 1$, osv.

Hvis dere vil vise påstanden min, som jeg overlater som en oppgave, må dere argumentere for at ting i $\mathbb{Z}/(p)$ har en invers hvis og bare hvis p er et primtall. Merk dere at en hindring til å ha en invers er dersom $a \cdot b = 0$ men hverken a eller b er 0. Dette skjer f.eks. i $\mathbb{Z}/(4)$, hvor $2 \cdot 2 = 0$, men $2 \neq 0$.