UPPSALA UNIVERSITET

Algebraiska Strukturer

Tentamen 2022-06-07 Lösningsförslag

Rami Abou Zahra

Inlämningsdatum
June 24, 2022

Contents

1. 5 snabba

1.1. Icke kommutativ ring. Vi påminner oss om en icke kommutativ ring:

Theorem 1.1: Icke-Kommutativ ring

En icke-kommutativ ring är en ring sådant att $\forall a, b \in R \quad a \cdot_R b \neq b \cdot_R a$

Då vektorrum är en ring, vars multiplikativa operator är matrismultiplikation och element är matriser, gäller det att en matris $\forall A, B \in V \quad A \times B \neq B \times A$

1.2. Kommutativ ring, ej integritetsområde.

Vi påminner oss om definitionen av ett integritetsområde:

Theorem 1.2: Integritetsområde

En ring R kallas för ett *integritetsområde* om

$$\forall a, b \neq 0 \in R \quad a \cdot_R b = b \cdot_R a \neq 0$$

De kommutativa ringarna vi känner til är förstås $\mathbb{Z}$, men även $\mathbb{Z}_n$. Låt oss titta närmare på $\mathbb{Z}_n$.

I $\mathbb{Z}_n$ gäller $\forall a \in \mathbb{Z}_n \quad a \cdot n = n \cdot a = \bar{0}$, alltså har vi funnit en nolldelare! Alltså är $\mathbb{Z}_n$ inte ett integritetsområde, trots att det är en ring.

1.3. Euklidisk ring, ej kropp.

De fina egenskaperna hos en kropp är att varje nollskillt element har en invers sådant att med ringmultiplikationen fås en multiplikativ identitet. Då räcker det med att hitta en ring med nolldelare som är en Euklidisk ring, alltså gäller även $\mathbb{Z}_n$ här, men! Vi måste kräva att $n \neq p$ där p är ett primtal, annars är det en kropp!

1.4. Irreducibelt polynom i $\mathbb{Z}[x]$ grad 2.

Låt oss påminna oss om definitionen av reducibel:

Theorem 1.3: Irreducibelt element

Ett element icke-inverterbart element a i en ring R kallas för *irreducibelt* om $a = b \cdot_R c$ där b eller c är inverterbart.

Definitionen följer med även i polynomringar. Kom ihåg, 1_R är alltid inverterbart och en faktor i alla element.

Vi återgår nu till ringen vi är i, $\mathbb{Z}[x]$. Notera att $\mathbb{Z}$ är en kropp, och därmed gäller faktorsatsen. Tag därför ett polynom av grad 2 som inte har rötter i $\mathbb{Z}[x]$, det lättaste valet man kan göra är att välja ett komplext polynom, exempelvis $x^2 + 1$

1.5. **Eulers sats.**

Detta är inget annat än att formulera definitionen:

Theorem 1.4: Eulers sats

Låt $\text{sgd}(a, b) = 1$, då gäller $a^{\varphi(b)} \equiv 1 \mod b$

2. Låt R vara ett integritetsområde

2.1. **Definiera maximalt ideal.**

Här krävs inget annat än den rena definitionen, som lyder enligt följande:

Theorem 2.1: Maximalt ideal

Maximalt ideal är ett ideal $I \subseteq R$ sådant $\nexists P \subseteq R \wedge I \subseteq P$ där $P \neq R$

2.2. **Irreducibelt.**

Definitionen har skrivits i Theorem 1.3 (ja, det är ok att göra så på tentamen).

2.3. **Visa nollskillt och irreducibelt.**

Notera att denna fråga är lite mer ”dominant” än de andra, den vill att vi skall visa något. Då hjälper det att skriva upp vad vi vet för att sedan klura ut om vi minns någon sats som gör att pusselbitarna faller på plats:

- R integritetsområde $\Rightarrow$ R kropp
- Maximalt ideal genererat av $a \in R$
- Varje växande kedja av ideal konvergerar i ett integritetsområde
- Det finns ”triviala ideal”
- Ideal får ej vara tomma mängden (eller var det icke-tom? Tips! Tänk på kroppar, vilka är de triviala idealen?)
- Integritetsområde har inga nolldelare
- Kroppar har bara triviala ideal
- Ett irreducibelt element är icke-inverterbart

Nu har vi verktyg i vår verktygslåda vi kan arbeta mer med! Vi ser om vi kan bryta ner det vi vill visa i mindre bitar.

Vi vill visa att a är nollskillt. Vi noterar att vi är i ett integritetsområde, alltså kan ej a vara nolldelare. Vi söker alltså motsägelse till $\forall b \in R \quad a \cdot_R b \neq 0$. Vi leker lite med tanken med maximalt ideal, det är alltså det största idealet i ringen, generatorn kan väl inte vara noll? Hmm, vad händer om den är nollan? Då måste ringen vara $\{0\}$, men då kan vi inte vara i ett integritetsområde.
Vi har en plan! Vi skall nu försöka översätta detta till ett mer matematiskt språk:
Antag $a = 0$. Då är idealet som genereras av $a = \{a \cdot r | r \in R\} = \{0\}$. Idealet är maximalt, vilket betyder att idealet som genereras av den multiplikativa identiteten är *mindre* än idealet som genereras av 0. Detta kan inte stämma, eftersom det idealet är ett av de triviala idealen, nämligen ringen R!. Vi har visat att $R \subseteq \{0\}$, motsägelse, alltså gäller $a \neq 0$.

Nu vill vi visa att a är irreducibelt, vi måste först visa att a är icke-inverterbart. Om a är inverterbart finns det ett b sådant att $a \cdot_R b = 1_R$, men då skulle idealet som genereras vara hela ringen. Däremot motsäger detta antaganden, ty i uppgiften stod det att det finns *ett* a, men om a är inverterbart finns det ju ett b som också genererar idealet!