Konzept einer Algebra Vorlesung

1)
2)
3)
4)
5)
6)
7)
8)
9)
10)
11)
12)
13)
14)
15)
16)
17)
18)
19)
20)
21)

2 x wöchentlich ~ 25 Vorlesungen

Konzept einer Algebra Vorlesung

1) Isomorphiesätze
2) Sylowsätze
3) Klassengleichung
4) Auflösbarkeit
5) Sym. Gruppen
6)
7)
8)
9)
10)
11)
12)
13)
14)
15)
16)
17)
18)
19)
20)
21)

2 × wöchentlich ~ 25 Vorlesungen

Konzept einer Algebra Vorlesung

1) Isomorphiesätze
2) Sylowsätze
3) Klassengleichung
4) Auflösbarkeit
5) Sym. Gruppen
6) Grundlagen
7) Teilbarkeit I
8) Teilbarkeit II
9) Polynomringe I
10) Polynomringe II
11)
12)
13)
14)
15)
16)
17)
18)
19)
20)
21)

2 × wöchentlich ~ 25 Vorlesungen

Konzept einer Algebra Vorlesung

1) Isomorphiesätze
2) Sylowsätze
3) Klassengleichung
4) Auflösbarkeit
5) Sym. Gruppen
6) Grundlagen
7) Teilbarkeit I
8) Teilbarkeit II
9) Polynomringe I
10) Polynomringe II
11) Grundlagen
12) Körpererweit. I
13) Körpererweit. II
14) End. Körper
15)
16)
17)
18)
19)
20)
21)

2 × wöchentlich ~ 25 Vorlesungen

Konzept einer Algebra Vorlesung

1) Isomorphiesätze
2) Sylowsätze
3) Klassengleichung
4) Auflösbarkeit
5) Sym. Gruppen
6) Grundlagen
7) Teilbarkeit I
8) Teilbarkeit II
9) Polynomringe I
10) Polynomringe II
11) Grundlagen
12) Körpererweit. I
13) Körpererweit. II
14) End. Körper
15) Galoiserweit. I
16) Galoiserweit. II
17) Galoistheorie I
18) Galoistheorie II
19)
20)
21)

2 × wöchentlich ~ 25 Vorlesungen

Konzept einer Algebra Vorlesung

1) Isomorphiesätze
2) Sylowsätze
3) Klassengleichung
4) Auflösbarkeit
5) Sym. Gruppen
6) Grundlagen
7) Teilbarkeit I
8) Teilbarkeit II
9) Polynomringe I
10) Polynomringe II
11) Grundlagen
12) Körpererweit. I
13) Körpererweit. II
14) End. Körper
15) Galoiserweit. I
16) Galoiserweit. II
17) Galoistheorie I
18) Galoistheorie II
19) Einheitswurzeln
20) Auflösung von Gleichungen
21) Zirkel + Lineal

2 × wöchentlich ~ 25 Vorlesungen

Konzept einer Algebra Vorlesung

1) Isomorphiesätze
2) Sylowsätze
3) Klassengleichung
4) Auflösbarkeit
5) Sym. Gruppen
6) Grundlagen
7) Teilbarkeit I
8) Teilbarkeit II
9) Polynomringe I
10) Polynomringe II
11) Grundlagen
12) Körpererweit. I
13) Körpererweit. II
14) End. Körper
15) Galoiserweit. I
16) Galoiserweit. II
17) Galoistheorie I
18) Galoistheorie II
19) Einheitswurzeln
20) Auflösung von Gleichungen
21) Zirkel + Lineal

2 × wöchentlich ~ 25 Vorlesungen → + etwas Module Theorie

Vorlesung 8 Teilbarkeit II

Letztes Mal: $\mathbb{Z}$, Euklid und Bézout

$1071 = 1 \cdot 1029 + 42$

$1029 = 24 \cdot 42 + 21$

$42 = 2 \cdot 21$

$\Rightarrow ggT = 21$

$ggT = 1 \Rightarrow 1 \in (a, b)$

$ggT(6, 13) = 1$

$1 = -2 \cdot 6 + 1 \cdot 13$

Heute: Die Verallgemeinerung!

Hauptbeispiele
- $\mathbb{Z}$
- $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Definition 8.1 Ein Integritätsring R heißt euklidisch (oder Euklidische Ring) falls es eine Gradabbildung

$$\delta : R^* \to \mathbb{N}^*$$

so gibt, dass

$$\forall a, b \in R \setminus \{0\} \; \exists r, q \in R \text{ mit } b = qa + r \text{ und } \delta(r) < \delta(a) \text{ oder } r = 0$$

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Definition 8.1 Ein Integritätsring R heißt euklidisch (oder Euklidische Ring) falls es eine Gradabbildung

$$\delta : R^* \to \mathbb{N}^*$$

so gibt, dass

$$\forall a, b \in R \; \exists r, q \in R \text{ mit } b = qa + r$$
$$\overset{!!}{0} \text{ und } \delta(r) < \delta(a) \text{ oder } r = 0$$

Das heißt es gilt der Euklidische Algorithmus

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Beispiel 8.2

- $\mathbb{Z}$ mit $\delta(a) = |a|$
- $\mathbb{Q}[x]$ mit $\delta(p) = \text{grad}(p)$
- $\mathbb{K}[x]$ für jeden Körper $\mathbb{K}$
- $\mathbb{Z}[i]$ mit $\delta(a+ib) = a^2+b^2$
- Kein Beispiel $\mathbb{Z}[\sqrt{-5}]$ (warum sehen wir gleich)

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Proposition 8.3 (Bézout)

Jeder euklidische Ring ist ein Hauptidealring.

Beweis: Sei $I \neq \{0\}$ ein Ideal.

Wähle $a \in I$ mit $\delta(a)$ minimal.

Dann: $\forall b \in I \; \exists q \in R$ mit $a = qb$. $\square$

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Proposition 8.3 (Bézout)

Jeder euklidische Ring ist ein Hauptidealring.

Beweis: Sei $I \neq \{0\}$ ein Ideal.

Wähle $a \in I$ mit $\delta(a)$ minimal.

Dann: $\forall b \in I \; \exists q \in R$ mit $a = qb$. $\square$

[Nichtkonstruktiv.

Übungsaufgabe: Für $a, b \in I$ ist $\operatorname{ggT}(a,b)$ der Erzeuger von I.

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Was mögen wir noch an $\mathbb{Z}$?

Die Primfaktorzerlegung!

Zur Erinnerung:

- Prim in Ringen $p \mid ab \Rightarrow p \mid a \vee p \mid b$
- Irreduzibel $p = ab \Rightarrow a$ oder b Einheit
- In Hauptidealringen

Irreduzibel = Prim

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Definition 8.4

Ein Integritätsring R heißt faktoriell, wenn sich jede nicht-Einheit als Produkt von Primelementen schreiben lässt.

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Definition 8.4

Ein Integritätsring R heißt faktoriell, wenn sich jede nicht-Einheit als Produkt von Primelementen schreiben lässt.

↳ Lemma 8.5 Irreduzibel $\Rightarrow$ Prim. Beweis: Gleich

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Beispiel 8.5

```
In[17]:= p = 12 + 34 x + 34 x^2 + 14 x^3 + 2 x^4;
         q = 432 + 396 x + 132 x^2 + 19 x^3 + x^4;
         r = 1 + x^2;

In[20]:= PolynomialGCD[p, q]
         PolynomialGCD[p, r]
         PolynomialGCD[q, r]

Out[20]= 3 + x

Out[21]= 1

Out[22]= 1

In[35]:= PolynomialLCM[p, q] // Expand
         PolynomialLCM[p, r] // Expand
         PolynomialLCM[q, r] // Expand

Out[35]= 1728 + 5904 x + 7944 x^2 + 5428 x^3 + 2042 x^4 + 426 x^5 + 46 x^6 + 2 x^7

Out[36]= 12 + 34 x + 46 x^2 + 48 x^3 + 36 x^4 + 14 x^5 + 2 x^6

Out[37]= 432 + 396 x + 564 x^2 + 415 x^3 + 133 x^4 + 19 x^5 + x^6

In[26]:= Factor[p]
         Factor[q]
         Factor[r]

Out[26]= 2 (1 + x)^2 (2 + x) (3 + x)

Out[27]= (3 + x) (4 + x) (6 + x)^2

Out[28]= 1 + x^2

In[29]:= Factor[p, GaussianIntegers → True]
         Factor[q, GaussianIntegers → True]
         Factor[r, GaussianIntegers → True]

Out[29]= 2 (1 + x)^2 (2 + x) (3 + x)

Out[30]= (3 + x) (4 + x) (6 + x)^2

Out[31]= (-i + x) (i + x)
```

- $\mathbb{Z}$
- $\mathbb{Q}[x]$
- $\mathbb{K}[x]$
- $\mathbb{Z}[i]$
- Kein Beispiel $\mathbb{Z}[\sqrt{-5}]$

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Beispiel 8.5

```
In[17]:= p = 12 + 34 x + 34 x^2 + 14 x^3 + 2 x^4;
         q = 432 + 396 x + 132 x^2 + 19 x^3 + x^4;
         r = 1 + x^2;

In[20]:= PolynomialGCD[p, q]
         PolynomialGCD[p, r]
         PolynomialGCD[q, r]

Out[20]= 3 + x

Out[21]= 1

Out[22]= 1

In[35]:= PolynomialLCM[p, q] // Expand
         PolynomialLCM[p, r] // Expand
         PolynomialLCM[q, r] // Expand

Out[35]= 1728 + 5904 x + 7944 x^2 + 5428 x^3 + 2042 x^4 + 426 x^5 + 46 x^6 + 2 x^7

Out[36]= 12 + 34 x + 46 x^2 + 48 x^3 + 36 x^4 + 14 x^5 + 2 x^6

Out[37]= 432 + 396 x + 564 x^2 + 415 x^3 + 133 x^4 + 19 x^5 + x^6

In[26]:= Factor[p]
         Factor[q]
         Factor[r]

Out[26]= 2 (1 + x)^2 (2 + x) (3 + x)

Out[27]= (3 + x) (4 + x) (6 + x)^2

Out[28]= 1 + x^2

In[29]:= Factor[p, GaussianIntegers → True]
         Factor[q, GaussianIntegers → True]
         Factor[r, GaussianIntegers → True]

Out[29]= 2 (1 + x)^2 (2 + x) (3 + x)

Out[30]= (3 + x) (4 + x) (6 + x)^2

Out[31]= (-i + x) (i + x)
```

- $\mathbb{Z}$
- $\mathbb{Q}[x]$
- $\mathbb{K}[x]$
- $\mathbb{Z}[i]$

} Übungsaufgaben in Mathematica

- Kein Beispiel $\mathbb{Z}[\sqrt{-5}]$

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Gegenbeispiel 8.6

In $\mathbb{Z}[\sqrt{-5}]$ gilt:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$\Rightarrow 2 \mid 6$ aber $2 \nmid (1+\sqrt{-5})$

und $2 \nmid (1-\sqrt{-5})$

$\Rightarrow$ 2 ist nicht prim.

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Gegenbeispiel 8.6

In $\mathbb{Z}[\sqrt{-5}]$ gilt:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Aber 2 ist irreduzible

(Übungsaufgabe)

also ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Theorem 8.7

Euklidisch => Hauptidealring => Faktoriell

$\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{K}[x]$
$\mathbb{Z}[i]$

$\mathbb{Z}[\sqrt{-5}]$

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$

Vorlesung 8 Teilbarkeit II

Theorem 8.7

Euklidisch => Hauptidealring => Faktoriell

$\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{K}[x]$
$\mathbb{Z}[i]$
Sind alles

$\mathbb{Z}[\sqrt{-5}]$

Ist keins

Hauptbeispiele
- $\mathbb{Z}$ - $\mathbb{Z}[\sqrt{-5}]$
- $\mathbb{Q}[x]$