Übersicht
Vorlesungswoche 3

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Erinnerung

Integritätsringe R komm Ring, $R \neq 0$, $\boxed{xy = 0 \Rightarrow x = 0 \text{ oder } y = 0}$

Teilbarkeit $a \mid b \iff \exists\, c \in R:\ b = c \cdot a \iff b \in (a)$

Euklidische Ringe, Hauptidealringe

Integritätsring, in dem jedes Ideal Hauptideal wird

"Division mit Rest"

Irreduzible und prime Elemente

$p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.

$p \in R \setminus (R^\times \cup \{0\})$, $p = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$

Faktorielle Ringe

R Integritätsring

R faktoriell : jedes Elem von $R \setminus \{0\}$ lässt sich als Produkt von Primelementen schreiben

Jeder HIR ist faktoriell, insbes.: $\mathbb{Z}$

$\boxed{K[X] \quad (K \text{ Körper}).}$

Nullstellen von Polynomen

K Körper

$f \in K[X]$

$\alpha \in K$ Nullstelle von f $\Longleftrightarrow$ $f(\alpha) = 0$ $\Longleftrightarrow$ $(X - \alpha) \mid f$

$\exists g: \quad f = (X - \alpha) \cdot g$

Der chinesische Restsatz

Seien R ein Integritätsring und $a_1, \ldots, a_r \in R$, so dass $(a_i, a_j) = R$ für alle $i \neq j$. Sei $a = a_1 \cdot \cdots \cdot a_r$.

Seien $b_1, \ldots, b_r \in R$. Dann existiert ein Element $b \in R$, so dass

$$b \equiv b_i \mod a_i \quad \text{für alle } i = 1, \ldots, r$$

gilt.

$b - b_i \in (a_i)$

Äquivalenzrelationen

Relation auf X ist Teilmenge $R \subseteq X \times X$

Schreibe $x \sim y \iff (x,y) \in R$

R heißt Äquivalenzrelation, falls

$x \sim x \quad \forall x \in X$

$x \sim y \iff y \sim x \quad \forall x, y \in X$

$x \sim y,\ y \sim z \implies x \sim z.$

Bsp „$=$“.

Der Quotientenkörper eines Integritätsrings

$\mathbb{Z} \rightsquigarrow \mathbb{Q} = \left\{ \frac{a}{b} \; ; \; a, b \in \mathbb{Z}, \; b \neq 0 \right\}$ $\qquad \frac{a}{b} = \frac{c}{d} \iff ad = bc$

$$\begin{array}{ccc} \mathbb{Q} & \ni & \frac{a}{1} \\ \cup & & \uparrow \\ \mathbb{Z} & \ni & a \end{array}$$

R Integritätsring $\rightsquigarrow \mathrm{Quot}(R) = \left\{ \frac{a}{b} \; ; \; a, b \in R, \; b \neq 0 \right\}$

$$\begin{array}{ccc} \mathrm{Quot}(R) & & \frac{a}{1} \\ \uparrow & & \uparrow \\ R & & a \end{array}$$

$\frac{a}{b} = \frac{c}{d} \iff ad = bc$

$+, \cdot$

Faktorielle Ringe
Vorlesungswoche 3

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Zerlegung in irreduzible Elemente in Hauptidealringen

Satz Sei R ein Hauptidealring, $a_0 \in R \setminus (R^\times \cup \{0\})$.

Dann lässt sich a_0 als Produkt von irreduziblen Elementen schreiben.

äquiv: von Primelem.

Beweis Andernfalls können wir $a_0 = a_1 b_1$ mit $a_1, b_1 \in R \setminus (R^\times \cup \{0\})$ und so dass a_1 kein Produkt von irred.

(denn a_0 kann nicht irred. sein).

Dann $a_1 = a_2 b_2$ mit $a_i, b_i \in R \setminus (R^\times \cup \{0\})$, s.d. a_i kein Produkt von irred. Elem.

und so weiter: $a_i = a_{i+1} b_{i+1}$

Dann gilt also $a_1 \mid a_0$, $a_2 \mid a_1$, $a_3 \mid a_2$ ...

und jeweils $a_i \nmid a_{i+1}$ ..

Mit anderen Worten: $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$

Das ist nicht möglich, wie das folgende Lemma zeigt.

Idealketten in Hauptidealringen

<u>Lemma</u> Sei R ein Hauptidealring. Sei

$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ eine Kette von Idealen in R.

Dann existiert $i \geq 0$, so dass für alle $j \geq i$ gilt: $\mathfrak{a}_i = \mathfrak{a}_j$.

Quiz: Idealketten in $\mathbb{Z}$; in $K[X]$ (K Körper)

Formulieren Sie die Aussage des Lemmas für den Ring $\mathbb{Z}$ als Teilbarkeitsaussage in $\mathbb{Z}$. Warum ist sie richtig?

Sei K ein Körper. Formulieren Sie die Aussage des Lemmas für den Ring $K[X]$ als Teilbarkeitsaussage in $K[X]$. Warum ist sie richtig?

Quiz: Idealketten in $\mathbb{Z}$; in $K[X]$ (K Körper)

Formulieren Sie die Aussage des Lemmas für den Ring $\mathbb{Z}$ als Teilbarkeitsaussage in $\mathbb{Z}$. Warum ist sie richtig?

Sind $a_n \in \mathbb{Z}$, $n = 0, 1, 2, \ldots$ mit $a_{n+1} \mid a_n$ $\forall n$, dann ex. i, so dass $|a_i| = |a_j|$ für alle $j \geq i$.

Begründung: Aus der Voraussetzung folgt $|a_0| \geq |a_1| \geq \ldots$, diese Kette natürlicher Zahlen muss „enden"

Sei K ein Körper. Formulieren Sie die Aussage des Lemmas für den Ring $K[X]$ als Teilbarkeitsaussage in $K[X]$. Warum ist sie richtig?

Sind $f_n \in K[X]$, $n = 0, 1, 2, \ldots$ mit $f_{n+1} \mid f_n$ $\forall n$, dann ex. i, so dass $f_i = u_j f_j$ $(u_j \in K^\times)$ für alle $j \geq i$.

Begr. Es ist $\deg(f_{n+1}) \leq \deg(f_n)$ und $f_j \mid f_i$, $\deg(f_j) = \deg(f_i) \Rightarrow f_i, f_j$ assoziiert.

Idealketten in Hauptidealringen

<u>Lemma</u> Sei R ein Hauptidealring. Sei

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$ eine Kette von Idealen in R.

Dann existiert $i \geq 0$, so dass für alle $j \geq i$ gilt: $\mathfrak{a}_i = \mathfrak{a}_j$.

<u>Beweis</u> Sei $\mathfrak{a} = \bigcup_{n \geq 0} \mathfrak{a}_n$. Dann ist $\mathfrak{a} \subseteq R$ ein Ideal.

Weil R ein HIR ist, gibt es $a \in R$ mit $\mathfrak{a} = (a)$. Sei $i \in \mathbb{N}$ mit $a \in \mathfrak{a}_i$. Dann gilt für alle $j \geq i$:

$$(a) \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}_j \subseteq \mathfrak{a} = (a).$$ Also gilt überall "$=$".

Eindeutigkeit der Zerlegung

Lemma R Integritätsring, $p_1, \dots, p_r \in R$ Primelem., $q_1, \dots, q_s \in R$ irred. Elem.

Es gelte $p_1 \cdots p_r = q_1 \cdots q_s$.

Dann gilt $r = s$ und nach eventueller Umnummerierung der q_i

gilt für alle i, dass p_i und q_i zueinander assoziiert sind.

Beweis Vorbem. $p \in R$ prim, $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$,

per Induktion: $p \mid a_1 \cdots a_n \Rightarrow$ es ex i: $p \mid a_i$.

Nun gilt $p_1 \mid p_1 \cdots p_r = q_1 \cdots q_s$, also OE $p_1 \mid q_1$

Dann $q_1 = u_1 p_1$, $u_1 \in R$, sogar $u_1 \in R^\times$ weil q_1 irreduzibel.

Insbes.: p_1, q_1 zueinander assoziiert.

Aufheben: $p_1 \cdots p_r = u_1 p_1 \cdot q_2 \cdots q_s$,

also $p_2 \cdots p_r = \underbrace{(u_1 q_2)}\, q_3 \cdots q_s$ $\xrightarrow[\text{nach } r]{\text{Induktion}}$ Hier gilt Beh. des Lemmas.

alle Faktoren prim

alle Faktoren irred.

Faktorielle Ringe

Def. Ein Integritätsring R heißt faktoriell, wenn sich jedes Element aus $R \setminus (R^\times \cup \{0\})$ als Produkt von Primelementen schreiben lässt. (notwendigerweise eind. im Sinne des vorherigen Lemmas)

In diesem Fall (R faktoriell) ist jedes irred. Elem $p \in R$ ein Primelement.

Haben insgesamt bewiesen: Jeder Hauptidealring ist faktoriell.

Quiz / Beispiel: $\mathbb{Z}$

Quiz / Beispiel: $\mathbb{Z}$

Es ist $\mathbb{Z}^\times = \{1, -1\}$.

$a \neq 0$

Also: für jede ganze Zahl $a \in \mathbb{Z}$ existieren

$\varepsilon \in \{1, -1\}$ und Primzahlen $p_1, \ldots, p_r \in \mathbb{N}$

mit $a = \varepsilon \, p_1 \cdot \ldots \cdot p_r$

Dabei ist ε eindeutig bestimmt, und die p_i sind eindeutig bestimmt bis auf die Reihenfolge.

Quiz / Beispiel: $K[X]$

Quiz / Beispiel: $K[X]$

K Körper, $R = K[X]$, $R^\times = K^\times$

Ist $f \in K[X] \setminus \{0\}$, dann existieren $r \geq 0$, $u \in K^\times$ und normierte irreduzible Polynome $f_1, \dots, f_r$, so dass $f = u \cdot f_1 \cdot \ldots \cdot f_r$.

Dabei ist u eindeutig bestimmt, und die f_i sind eindeutig bestimmt bis auf die Reihenfolge.

Nullstellen von Polynomen
Vorlesungswoche 3

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Nullstellen von Polynomen

Sei R ein kommutativer Ring.

Ein Element $\alpha \in R$ heißt Nullstelle eines Polynoms $f \in R[X]$,

wenn $f(\alpha) = 0$.

Charakterisierung durch Teilbarkeitsbedingung

Sei R ein Integritätsring.

<u>Lemma</u> Sei $f \in R[X]$. Dann ist $\alpha \in R$ ist genau dann eine Nullstelle von f, wenn $(X-\alpha) \mid f$.

<u>Beweis</u> Wenn f ein Vielfaches ist von $X-\alpha$, etwa $f = (X-\alpha)\cdot g$, dann gilt $f(\alpha) = (\alpha-\alpha)\cdot g(\alpha) = 0$.

Gelte nun $f(\alpha)=0$. Wir schreiben $f = (X-\alpha)\cdot q + r$ mit $q, r \in R[X]$ und $\deg r < \deg(X-\alpha) = 1$.

$\boxed{\deg r < 1}$

Einsetzen von α: $0 = f(\alpha) = (\alpha-\alpha)\cdot q(\alpha) + r(\alpha) = r(\alpha) = \underset{R}{\underset{\cap}{r}}$

Also gilt $r=0$ und damit $f = (X-\alpha)\cdot q$.

Vielfachheit einer Nullstelle

R Integritätsring

Seien $f \in R[X] \setminus \{0\}$, $\alpha \in R$.

Dann sei $\mathrm{mult}_\alpha(f)$ die eind. bestimmte natürliche Zahl $m \in \mathbb{N}$, so dass $(X-\alpha)^m \mid f$ aber $(X-\alpha)^{m+1} \nmid f$.

Dann gilt α Nullstelle von $f \iff \mathrm{mult}_\alpha(f) > 0$.

und dann heißt $\mathrm{mult}_\alpha(f)$ die Multiplizität / Vielfachheit der Nullstelle α.

Wir sagen, $f \in R[X]$ zerfällt vollständig in Linearfaktoren, wenn sich f als Produkt von Polynomen vom Grad 1 schreiben lässt.

Quiz

Bestimmen Sie alle Nullstellen des Polynoms

$$f = (2X - 1)^2 \, (X^2 + X - 1)$$

und ihre Vielfachheiten.

Welches ist der kleinste Ring in der Kette

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

über dem f vollständig in Linearfaktoren zerfällt?

Quiz

Bestimmen Sie alle Nullstellen des Polynoms

$$4 \cdot (X-\tfrac{1}{2})^2 \cdot \left(X+\tfrac{1}{2}-\tfrac{\sqrt{5}}{2}\right)\left(X+\tfrac{1}{2}+\tfrac{\sqrt{5}}{2}\right) \in \mathbb{R}[X]$$

$$\parallel$$

$$f = (2X-1)^2 \cdot (X^2+X-1) \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X]$$

und ihre Vielfachheiten.

- in $\mathbb{Z}$: keine Nullstellen
- in $\mathbb{Q}$: $\frac{1}{2}$ doppelte Nullstelle: $\mathrm{mult}_{\frac{1}{2}}(f) = 2$
- in $\mathbb{R}$: $\frac{1}{2}$ dopp. Nullstelle, $-\frac{1}{2}+\frac{\sqrt{5}}{2}$, $-\frac{1}{2}-\frac{\sqrt{5}}{2}$ einfache Nullst.
- in $\mathbb{C}$: wie in $\mathbb{R}$

Welches ist der kleinste Ring in der Kette

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

über dem f vollständig in Linearfaktoren zerfällt? $\rightarrow$ $\mathbb{R}$

Der Fundamentalsatz der Algebra

Def. Ein Körper K heißt <u>algebraisch abgeschlossen</u>, wenn jedes (nicht-konstante) Polynom $\in K[X]$ vollständig in Linearfaktoren zerfällt.

<u>Bem</u> $\mathbb{Q}$, $\mathbb{R}$ <u>nicht</u> algebraisch abgeschlossen.

<u>Theorem</u> (Fundamentalsatz der Algebra)
Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Der Chinesische Restsatz
Vorlesungswoche 3

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Aufgabe (aus dem Buch *Sun-tzu Suan-ching*, 3. Jh.)

Gesucht ist eine Anzahl von Dingen. Wenn wir sie in Dreiergruppen aufteilen, bleiben 2 übrig. Wenn wir sie in Fünfergruppen aufteilen, bleiben 3 über. Wenn wir sie in Siebenergruppen aufteilen, bleiben 2 über. Wie viele Dinge sind es?

Gesucht $x \in \mathbb{N}$ mit

$$x \equiv 2 \mod 3$$

$$x \equiv 3 \mod 5$$

$$x \equiv 2 \mod 7$$

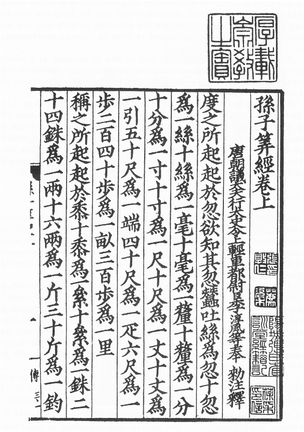

孫子算經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勑注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Abb. Wikipedia/public domain

Kongruenzen

R Integritätsring

Für $x, y, a \in R$ schreiben wir

$x \equiv y \mod a$ „x kongruent zu y modulo a",

wenn $a \mid (x - y)$.

Äquivalent: $x - y \in (a)$.

Erinnerung Ideale

Sei R ein kommutativer Ring

Dann gilt für $a, b \in R$: $\quad (a,b) = \{ xa + yb \, ; \; x, y \in R \}$

Also $\quad 1 \in (a,b) \iff (a,b) = R \iff$ es ex. $x, y \in R$:
$xa + yb = 1$.

Ist R ein Hauptidealring, dann ist $1 \in (a,b)$ dazu äquivalent,
dass 1 ein ggT von a, b ist.

Der chinesische Restsatz

Satz. Sei R ein Integritätsring. Seien $a_1, \ldots, a_r \in R$ mit $(a_i, a_j) = R$ für alle $i \neq j$.

Sei $a := a_1 \cdot \ldots \cdot a_r$.

Seien $b_1, \ldots, b_r \in R$. Dann existiert $b \in R$ mit

$$b \equiv b_i \mod a_i \quad \text{für } i = 1, \ldots, r. \qquad (*)$$

Sind b, b' Elemente, die beide die Kongruenzen $(*)$ erfüllen.

Dann gilt $b \equiv b' \mod a$.

$a_1, \ldots, a_r \in R$, $(a_i, a_j) = R$ $i \neq j$

Beweis für Hauptidealring R.

Vorüberlegung: Sei $a_i' := \prod_{j \neq i} a_j$. Dann gilt $(a_i, a_i') = R$.

Weil R HIR, gzz: $ggT(a_i, a_i') = 1$.

Das ist klar, weil R faktoriell ist.

Wir können also $1 = x_i a_i + \underbrace{y_i a_i'}$ schreiben, $x_i, y_i \in R$.

$$y_i a_i' \equiv \begin{cases} 0 & \text{mod } a_j, \ j \neq i. \\ 1 & \text{mod } a_i \end{cases}$$

Wir definieren $b := \sum_{i=1}^{r} \underbrace{b_i y_i a_i'}$

$$\equiv \begin{cases} 0 & \text{mod } a_j, \ j \neq i \\ b_i & \text{mod } a_i \end{cases}$$

gesucht: $b \in R$ mit

$b \equiv b_i \mod a_i$, $i = 1, \ldots, r$

Dann erfüllt b die vorgegebenen Kongruenzbedingungen.

Eindeutigkeitsaussage: Seien $b, b' \in R$ gegeben mit $b \equiv b_i \equiv b'$ mod a_i, $i = 1, \dots, r$.

Dann gilt $a_i \mid (b - b')$, und da die a_i paarweise teilerfremd sind, folgt $a = a_1 \cdots a_r \mid (b - b')$.

Quiz

Finden Sie alle $x \in \mathbb{Z}$ mit

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$$

Quiz

Finden Sie alle $x \in \mathbb{Z}$ mit

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$$

Vorbereitung:

$$1 = (-23) \cdot 3 + \boxed{2 \cdot 35}$$

$$1 = (-4) \cdot 5 + \boxed{1 \cdot 21}$$

$$1 = (-2) \cdot 7 + \boxed{1 \cdot 15}$$

$35 = 5 \cdot 7$

$21 = 3 \cdot 7$

$15 = 3 \cdot 5$

Eine Lösung:

$$x = 2 \cdot \boxed{2 \cdot 35} + 3 \cdot \boxed{1 \cdot 21} + 2 \cdot \boxed{1 \cdot 15} = \underline{233}$$

Lösungsmenge: $\{233 + 105k \,;\, k \in \mathbb{Z}\}$ $\qquad 105 = 3 \cdot 5 \cdot 7$

$$\left(= \{23 + 105k \,;\, k \in \mathbb{Z}\}\right)$$

Kleinste Lösung ≥ 0 : 23

Quiz

Finden Sie alle $x \in \mathbb{Z}$ mit

$$x \equiv 2 \mod 6, \qquad x \equiv 3 \mod 8.$$

Quiz

Finden Sie alle $x \in \mathbb{Z}$ mit

$$x \equiv 2 \mod 6, \qquad x \equiv 3 \mod 8.$$

Es gibt kein $x \in \mathbb{Z}$, das diese Bedingungen erfüllt,

denn

$$\left.\begin{aligned} x &\equiv 2 \mod 6 \quad \Rightarrow \quad x \equiv 0 \mod 2, \\ x &\equiv 3 \mod 8 \quad \Rightarrow \quad x \equiv 1 \mod 2 \end{aligned}\right\} \text{ ein Widerspruch!}$$

(Das widerspricht nicht dem Chinesischen Restsatz, denn 6 und 8 sind nicht teilerfremd!)

Äquivalenzrelationen
Vorlesungswoche 3

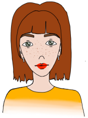
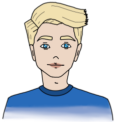
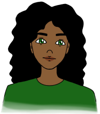
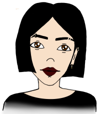
Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Relationen (zwischenmenschlich :-))

			
		X	
	X		

Abbildungen: Inga Görtz CC-BY

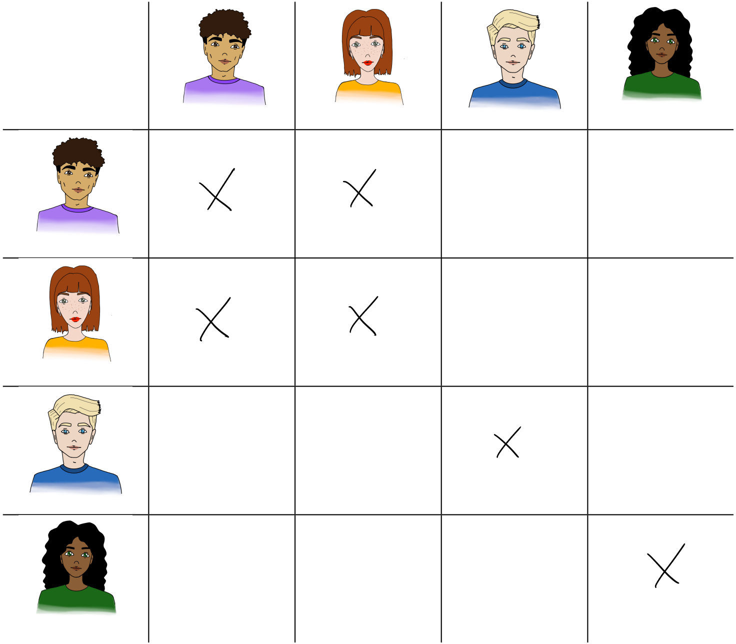


Abb. Inga Görtz CC-BY

Relationen (mathematisch)

Def. Eine Relation zwischen Mengen X und Y ist eine Teilmenge $R \subseteq X \times Y$.

Eine Relation auf einer Menge X ist eine Teilmenge $R \subseteq X \times X$.

Eigenschaften von Relationen

Sei X eine Menge, R eine Relation auf X.

Def.

(1) R heißt *reflexiv*, wenn: $\forall x \in X: \quad (x,x) \in R.$

(2) R heißt *symmetrisch*, wenn: $\forall x,y \in X: \quad (x,y) \in R$

$$\Longleftrightarrow (y,x) \in R$$

(3) R heißt *transitiv*, wenn $\forall x,y,z \in X: \quad (x,y), (y,z) \in R$

$$\Longrightarrow (x,z) \in R.$$

(4) R heißt *antisymmetrisch*, wenn $\forall x,y \in X:$

$$(x,y), (y,x) \in X \Longrightarrow x = y$$

Quiz

$\{(x,y) \in \mathbb{Z}\times\mathbb{Z};\ x \leq y\} \subseteq \mathbb{Z}\times\mathbb{Z}$

Kreuzen Sie an, welche Relation welche Eigenschaften hat. (Es sei R ein Integritätsring.)

	reflexiv	symmetrisch	transitiv	antisymmetrisch
$=$				
$\leq$ (auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$)				
$<$ (auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$)				
$\neq$				
$\mid$ (in R)				
assoziiert zu (in R)				
$\equiv$ (mod a für $a \in R$)				

Quiz

Kreuzen Sie an, welche Relation welche Eigenschaften hat. (Es sei R ein Integritätsring.)

	reflexiv	symmetrisch	transitiv	antisymmetrisch
$=$	✓	✓	✓	✓
$\leq$ (auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$)	✓	✗	✓	✓
$<$ (auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$)	✗	✗	✓	(✓)
$\neq$	✗	✓	✗	✗
$\mid$ (in R)	✓	✗	✓	✓
assoziiert zu (in R)	✓	✓	✓	✗
$\equiv$ (mod a für $a \in R$)	✓	✓	✓	✗

reflexiv + transitiv + antisymmetrisch: "partielle Ordnung"

Äquivalenzrelationen

Def. Sei X eine Menge. Eine Äquivalenzrelation auf X ist eine Relation $R \subseteq X \times X$ auf X, die reflexiv, symmetrisch und transitiv ist.

Schreibweise häufig: $x \sim y \iff (x,y) \in R$.

Bsp. $=$, assoziiert (in Integritätsring R), $\equiv \mod a$

Äquivalenzklassen

Sei $\sim$ eine Äquivalenzrelation auf der Menge X.

Def. Für $x \in X$ heißt $\{ y \in X ; \; y \sim x \} = [x] \quad (\subseteq X)$

die <u>Äquivalenzklasse von x</u>.

Sind $x, y \in X$, so gilt $\quad y \in [x] \iff [y] = [x]$.

$$(\text{'}\Rightarrow\text{'} \quad \subseteq \quad z \in [y] \Rightarrow z \sim y \underset{y \sim x}{\Longrightarrow} z \sim x \Rightarrow z \in [x]$$

$$\supseteq \quad z \in [x] \Rightarrow z \sim x \underset{x \sim y}{\Longrightarrow} z \sim y \Rightarrow z \in [y])$$

Folg: Sind $x, y \in X$, dann gilt $\quad [x] = [y]$ oder $[x] \cap [y] = \emptyset$.

Beweis Wenn $z \in [x] \cap [y]$, dann $[x] = [z] = [y]$.

Die Menge der Äquivalenzklassen

X Menge,

$\sim$ Äquivalenzrelation

$X/\sim$ sei die Menge der Äquivalenzklassen.

$\rightsquigarrow$ Haben surjektive Abb.

$$\begin{aligned} X &\longrightarrow X/\sim \\ x &\longmapsto [x] \end{aligned}$$

<u>Beispiel</u> $X = \mathbb{Z}$, $n \in \mathbb{N}_{>1}$, $x \sim y :\Longleftrightarrow x \equiv y \mod n$

$\rightsquigarrow$ $X/\sim$ "$=$" $\mathbb{Z}/n$ $\quad (= \{ \bar{0}, \bar{1}, \dots, \overline{n-1} \})$

$\qquad \shortparallel$

$\{[0], [1], \dots, [n-1]\} = \{[1], \dots, [n-1], [n]\}$ $\quad$ (denn $[0] = [n]$)

Der Quotientenkörper eines Integritätsrings

Vorlesungswoche 3

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

$\mathbb{Z}$ und $\mathbb{Q}$

$$\mathbb{Q} = \left\{ \frac{a}{b} \;;\; a, b \in \mathbb{Z},\; b \neq 0 \right\} \qquad \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

$$\| ?$$

$$\frac{a}{b} = \frac{a'}{b'},\; \frac{c}{d} = \frac{c'}{d'} \rightsquigarrow \frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd'+b'c'}{b'd'}$$

Bsp, was nicht funktioniert:

$$\left\{ \frac{a}{b} \;;\; a, b \in \mathbb{Z},\; b > 0 \right\}$$

$$\frac{a}{b} \diamond \frac{c}{d} := \frac{a+c}{b+d}$$

"nicht wohldefiniert"

Allgemeine Konstruktion

R Integritätsring

Sei $M := R \times (R \setminus \{0\})$

und betrachte auf M die Relation $(a,b) \sim (c,d) \iff ad = bc$.

Dies ist eine Äquivalenzrelation.

Sei $K := M/_\sim$ die Menge der Äquivalenzklassen.

Die Äquivalenzklasse von $(a,b) \in M$ bezeichnen wir mit $\frac{a}{b}$.

Definiere Rechenoperationen auf K wie folgt:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

(R Integritätsring, $b, d \neq 0 \Rightarrow bd \neq 0$)

Wohldefiniertheit der Rechenoperationen

zz: wenn $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$ $\quad$ ($a, b, a', b', c, d, c', d' \in R$, $b, b', d, d' \neq 0$)

dann $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, $\quad \frac{ac}{bd} = \frac{a'c'}{b'd'}$,

das bedeutet: $\quad ab' = a'b, \quad cd' = c'd \implies \begin{cases} (ad+bc)\,b'd' = (a'd'+b'c')\,bd \\ ac\,b'd' = bd\,a'c'. \end{cases}$

Körperaxiome

- $(K,+)$ kommutative Gruppe

  neutrales Element $\frac{0}{1}$ $\qquad \frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+0\cdot b}{b\cdot 1}$

  $$=\frac{a}{b}$$

  Negatives von $\frac{a}{b}$ ist $\frac{-a}{b}$

  $$\frac{a}{b}+\frac{-a}{b}=\frac{ab+(-a)b}{b^2}=\frac{0}{b^2}=\frac{0}{1}$$

  $$(\rightsquigarrow \quad -\frac{a}{b}=\frac{-a}{b} \qquad \left(=\frac{a}{-b}\right))$$

- $(K\setminus\{0\},\cdot)$ kommutative Gruppe, neutr. Elem. $\frac{1}{1}$, Inverse von $\frac{a}{b}$ $(\neq 0)$ ist $\frac{b}{a}$. $\left[\frac{a}{b}\neq 0 \Leftrightarrow a\neq 0\right]$

- Distributiv gesetz

Wir erhalten insgesamt einen Körper K, den sogenannten Quotientenkörper des Integritätsrings R.

Bezeichnung: $\mathrm{Quot}(R)$

Der natürliche Homomorphismus $R \to \mathrm{Quot}(R)$

R Integritätsring

Dann ist $R \longrightarrow \mathrm{Quot}(R)$, $a \longmapsto \frac{a}{1}$, ein injektiver Ringhomom.

(Ringhomom.: $\frac{a+b}{1} \overset{!}{=} \frac{a}{1} + \frac{b}{1}$ · $\frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$ · $\frac{1}{1} = 1_{\mathrm{Quot}(R)}$

injektiv: gzz, dass $\mathrm{Kern} = \{0\}$. $a \in R$, $\frac{a}{1} = 0 = \frac{0}{1} \Rightarrow a = a \cdot 1 = 0 \cdot 1 = 0$)

Quiz

„Beschreiben“ Sie möglichst gut die folgenden Quotientenkörper:

$\mathrm{Quot}(\mathbb{Z})$

$\mathrm{Quot}(\mathbb{C})$

$\mathrm{Quot}(\mathbb{Q}[X])$

$\mathrm{Quot}(R)$ (R ein faktorieller Ring)

Quiz

„Beschreiben“ Sie möglichst gut die folgenden Quotientenkörper:

$\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$

R Körper

$\rightsquigarrow R \to \mathrm{Quot}(R)$

Isomorphismus von Ringen

$\mathrm{Quot}(\mathbb{C}) = \mathbb{C}$ $\qquad \frac{a}{b} = ab^{-1} \quad (a, b \in \mathbb{C}, b \neq 0)$

$\mathrm{Quot}(\mathbb{Q}[X]) = \left\{ \frac{f}{g} \,;\, f, g \in \mathbb{Q}[X],\ g \neq 0 \right\}$

$\mathrm{Quot}(R)$ $\quad$ (R ein faktorieller Ring)

$P \subseteq R$ "Vertretersystem der Primelemente von R bis auf Assoziiertheit"

$$\mathrm{Quot}(R)^\times = \left\{ u \cdot \prod_{p \in P} p^{v_p} \;;\; \begin{array}{l} u \in R^\times, \\ v_p \in \mathbb{Z}, \\ \text{nur endlich viele} \\ v_p \neq 0 \end{array} \right\}$$