UNTERLAGEN ZUR MENGENLEHRE

VORLESUNG "KOMMUTATIVE ALGEBRA", SOMMERSEMESTER 2009

1. Geordnete Mengen

Eine *geordnete Menge* $(M, \leq)$ ist ein Paar aus einer Menge und einer Ordnungsrelation auf M. Die Relation ist $\leq$ ist eine *lineare Ordnung*, wenn für alle $x, y \in M$ gilt: $x \leq y$ oder $y \leq x$.

Definition 1.1. Eine geordnete Menge $(M, \leq)$ erfüllt die *Maximalbedingung*, wenn jede nichtleere Teilmenge von M ein maximales Element hat.

$(M, \leq)$ erfüllt also die Maximalbedingung, wenn

$$\forall N \subseteq M : N \neq \emptyset \Rightarrow \exists n \in N : (\forall x \in N : n \leq x \Rightarrow n = x).$$

gilt.

Definition 1.2. Eine geordnete Menge $(M, \leq)$ erfüllt die aufsteigende Kettenbedingung (ACC), wenn es keine injektive Funktion $f : \mathbb{N} \to M$ mit der Eigenschaft $f(i) < f(i+1)$ für alle $i \in \mathbb{N}$ gibt.

Wir setzen voraus, dass die Axiome der Zermelo-Fränkelschen Mengenlehre mit Auswahlaxiom erfüllt sind. Dann gelten folgende Sätze.

Satz 1.3. *Für eine geordnete Menge* $(M, \leq)$ *sind äquivalent:*

(1) $(M, \leq)$ *erfüllt die* (ACC).
(2) $(M, \leq)$ *erfüllt die Maximalbedingung.*

Satz 1.4 (Lemma von Zorn)**.** *Sei* $(M, \leq)$ *eine geordnete Menge. Wir nehmen an, dass jede linear geordnete Teilmenge* L *von* M *eine obere Schranke in* M *hat. (Das heißt, dass es für jede linear geordnete Teilmenge* L *ein* $m \in M$ *gibt, sodass für alle* $l \in L$ *die Relation* $l \leq m$ *gilt.) Dann besitzt* $(M, \leq)$ *ein maximales Element.*

Date: March 13, 2009.
Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, Austria, `erhard@algebra.uni-linz.ac.at`.

2. Kommutative Ring mit Eins

Definition 2.1. Eine Algebra $\langle R, +, -, \cdot, 0, 1\rangle$ ist ein *kommutativer Ring mit Eins*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und $0, 1$ Elemente aus R sind, sodass für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$
(2) $x + (-x) = 0$
(3) $(x + y) + z = x + (y + z)$
(4) $x + y = y + x$
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6) $(x + y) \cdot z = x \cdot z + y \cdot z$
(7) $x \cdot (y + z) = x \cdot y + x \cdot z$
(8) $1 \cdot x = x$
(9) $x \cdot 1 = x$
(10) $x \cdot y = y \cdot x$.

Definition 2.2. Sei R ein kommutativer Ring mit Eins. Eine nichtleere Teilmenge I von R ist ein *Ideal* von R, wenn für alle $r \in R$ und $i, j \in I$ gilt, dass $r \cdot i$ und $i + j$ in I sind.

Definition 2.3. Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Dann ist das *von A erzeugte Ideal* $\langle A\rangle_R$ definiert durch

$$\langle A\rangle_R := \bigcap\{I \mid I \text{ Ideal von } R \text{ und } A \subseteq I\}.$$

Satz 2.4. *Sei R ein kommutativer Ring mit Eins, und sei $A \subseteq R$. Dann gilt*

$$\langle A\rangle_R = \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}.$$

Definition 2.5. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Dann ist I *endlich erzeugt*, wenn es eine endliche Menge $A \subseteq R$ gibt, sodass $I = \langle A\rangle$.

Satz 2.6. *Sei R ein kommutativer Ring mit Eins, und sei $I(R)$ die Menge der Ideale von R. Dann sind äquivalent:*

(1) *$(I(R), \subseteq)$ erfüllt die* (ACC).
(2) *Jedes Ideal von R ist endlich erzeugt.*

Definition 2.7. Sei R ein kommutativer Ring mit Eins. R heißt *noethersch*, wenn jedes Ideal von R endlich erzeugt ist.

Definition 2.8. Sei R ein kommutativer Ring mit Eins. Ein Ideal I von R ist *maximal*, wenn $I \neq R$, und wenn es kein Ideal J mit $I \subseteq J \subseteq R$, $I \neq J$, $J \neq R$ gibt.

In einem noetherschen Ring ist jedes Ideal in einem maximalen Ideal enthalten. Aus dem Zornschen Lemma folgt, dass das sogar für alle kommutativen Ringe mit Eins gilt:

Satz 2.9. *Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Dann gibt es ein maximales Ideal M von R mit $I \subseteq M$.*

3. Satz von Ramsey

Sei X eine Menge, und sei p eine natürliche Zahl. Dann bezeichnen wir mit $\binom{X}{p}$ die Menge aller p-elementigen Teilmengen von X, also

$$\binom{X}{p} = \{Y \mid Y \subseteq X \text{ und } |Y| = p\}.$$

Satz 3.1. *Sei X eine unendliche Menge, und seien $p, t \in \mathbb{N}$. Sei $F : \binom{X}{p} \to \{1, \ldots, t\}$. Dann gibt es eine unendliche Teilmenge Y von X, sodass F auf $\binom{Y}{p}$ konstant ist.*

Beweis: Induktion nach p. Induktionsschritt: Sei $p \geq 2$, und sei F eine Färbung der p-elementigen Teilmengen von $\mathbb{N}$ mit t Farben. Für jedes $a \in \mathbb{N}$ definieren wir eine Färbung G_a der $(p-1)$-elementigen Teilmengen von $X \setminus \{a\}$ durch

$$G_a(M) := F(M \cup \{a\})$$

für alle $M \in \binom{X \setminus \{a\}}{p}$. Nun definieren wir eine Folge $(x_i)_{i \in \mathbb{N}_0}$ aus X, und eine Folge $(Y_i)_{i \in \mathbb{N}_0}$ von Teilmengen von X. Wir definieren $Y_0 := X$, und wählen x_0 als ein Element von X. Wir werden nun die Folgen $(x_i)_{i \in \mathbb{N}_0}$ und $(Y_i)_{i \in \mathbb{N}_0}$ so definieren, dass jedes Y_i eine unendliche Teilmenge von X ist, und dass $x_i \in Y_i$. Wir definieren die Folgen rekursiv. Sei dazu $i \in \mathbb{N}_0$. Da $Y_i \setminus \{x_i\}$ unendlich ist, gibt es nach Induktionsvoraussetzung eine unendliche Teilmenge Y_{i+1} von $Y_i \setminus \{x_i\}$, sodass alle $(p-1)$-elementigen Teilmengen von Y_{i+1} die gleiche Farbe unter der Färbung G_{x_i} haben. Das Element x_{i+1} wählen wir aus Y_{i+1}.

Wir betrachten nun die Menge

$$Z := \{x_i \mid i \in \mathbb{N}_0\}.$$

Für jede p-elementige Teilmenge A von Z definieren wir den *kleinsten Index in* A, $\operatorname{ind}(A)$, als das kleinste $j \in \mathbb{N}_0$, sodass $x_j \in A$. Wir zeigen nun:

$$\text{Für alle } A, B \in \binom{Z}{p} \text{ mit } \operatorname{ind}(A) = \operatorname{ind}(B) \text{ gilt } F(A) = F(B).$$

Sei dazu $i := \mathrm{ind}(A)$. Alle x_j mit $j > i$ liegen in Y_{i+1}. Folglich ist A eine Teilmenge von $Y_{j+1} \cup \{x_i\}$. Ebenso ist B eine Teilmenge von $Y_{j+1} \cup \{x_i\}$. Wegen der Konstruktion von Y_{j+1} ist $G_{x_i}(A \setminus \{x_i\}) = G_{x_i}(B \setminus \{x_i\})$. Also gilt $F(A) = F(B)$.

Nun betrachten wir die Abbildung $h : \mathbb{N}_0 \to \{1, \ldots, t\}$, die durch

$$h(i) := F(\{x_i, \ldots, x_{i+p-1}\})$$

für $i \in \mathbb{N}_0$ definiert ist. Es gibt eine unendliche Teilmenge J von $\mathbb{N}_0$, sodass $h|_J$ konstant ist. Wir behaupten nun, dass

$$Y := \{x_j \,|\, j \in J\}$$

die gewünschten Eigenschaften erfüllt.

Seien dazu C und D p-elementige Teilmengen von Y, und seien $c_1 < \cdots < c_p$ und $d_1 < \cdots < d_p$ so, dass $C = \{x_{c_1}, x_{c_2}, \ldots, x_{c_p}\}$ und $D = \{x_{d_1}, x_{d_2}, \ldots, x_{d_p}\}$. Da $\mathrm{ind}(C) = c_1 = \mathrm{ind}(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$, gilt

$$F(C) = F(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$$

und ebenso

$$F(D) = F(\{x_{d_1}, x_{d_1+1}, \ldots, x_{d_1+p-1}\}).$$

Also gilt $F(C) = h(c_1)$ und $F(D) = h(d_1)$. Da x_{c_1} in Y liegt, gilt $c_1 \in J$; ebenso gilt $d_1 \in J$, und folglich $h(c_1) = h(d_1)$. Also haben C und D die gleiche Farbe. $\square$

4. Results from order theory

Let $\mathbb{A} = (A, \leq)$ be a partially ordered set. We write $a||b$ if a and b are not comparable. We say that $\mathbb{A}$ satisfies the *descending chain condition* (DCC) if there is no infinitely descending chain $a_1 > a_2 > a_3 > \ldots$.

For $m \in \mathbb{N}$, we define a partially ordered set $\mathbb{A}^m = (A^m, \leq)$, where $\mathbf{a} \leq \mathbf{b}$ if for all $i \in \{1, \ldots, m\}$, we have $\mathbf{a}_i = \mathbf{b}_i$. We start with a well-known fact.

Lemma 4.1. *Let $\mathbb{A}$ be a partially ordered set with* (DCC) *such that all antichains of $\mathbb{A}$ are finite. Then $\mathbb{A}^m$ satisfies* (DCC)*, and all antichains of $\mathbb{A}$ are finite.*

Proof: Let $\langle \mathbf{a}^{(i)} \,|\, i \in \mathbb{N}\rangle$ be an infinite sequence of elements of A^m. We color each 2-element subset $\{i, j\}$ of $\mathbb{N}$ with $i < j$ with one of 3^m colors. As colors, we take the functions from $\{1, \ldots, m\}$ to $\{\leq, >, ||\}$. Now, for $i < j$ and $k \in \{1, \ldots, m\}$, we denote the k-th component of $\mathbf{a}^{(i)}$ by $\mathbf{a}_k^{(i)}$, and we define

$$C(\{i, j\})\,(k) := \begin{cases} \leq & \text{if } \mathbf{a}_k^{(i)} \leq \mathbf{a}_k^{(j)}, \\ > & \text{if } \mathbf{a}_k^{(i)} > \mathbf{a}_k^{(j)}, \\ || & \text{if } \mathbf{a}_k^{(i)} \;||\; \mathbf{a}_k^{(j)}. \end{cases}$$

By Ramsey's Theorem [Ramsey, 1929], $\mathbb{N}$ has an infinite subset T such that all 2-element subsets of T have the same color C. We will now show that $C(k) = \boldsymbol{\leq}$ for all $k \in \{1, \ldots, m\}$.

Seeking a contradiction, we suppose that there is a k such that $C(k) = \boldsymbol{>}$ or $C(k) = \boldsymbol{||}$. Let $t_1 \leq t_2 \leq t_3 \ldots$ be the elements of T. If $C(k) = \boldsymbol{>}$, we have

$$\mathbf{a}_k^{(t_1)} > \mathbf{a}_k^{(t_2)} > \mathbf{a}_k^{(t_3)} > \cdots,$$

contradicting the fact that $\mathbb{A}$ satisfies the (DCC). Similarly, $C(k) = \boldsymbol{||}$ yields an infinite antichain in $\mathbb{A}$.

Hence, every infinite sequence in $\mathbb{A}^m$ contains an infinite ascending chain. Therefore, $\mathbb{A}$ cannot have an infinite descending chain, nor an infinite antichain. $\square$

As a corollary, we obtain *Dickson's Lemma*.

Corollary 4.2 (cf. [Dickson, 1913, Lemma A])**.** *The ordered set $\langle \mathbb{N}_0^m, \leq \rangle$ has no infinite antichains.*

Definition 4.3. A subset I of $\mathbb{N}_0^m$ is an *upward closed set*[1] if for all $\mathbf{a} \in I$ and $\mathbf{b} \in \mathbb{N}_0^m$ with $\mathbf{a} \leq \mathbf{b}$, we have $\mathbf{b} \in I$.

For an upward closed set I, let $\mathcal{M}(I)$ be the set of minimal elements in I. For every subset M of $\mathbb{N}_0^m$, let $\mathcal{U}(M) := \{\mathbf{a} \in \mathbb{N}_0^m \mid \text{there is } \mathbf{z} \in M \text{ such that } \mathbf{z} \leq \mathbf{a}\}$. Clearly, $\mathcal{U}(M)$ is upward closed. Then we have:

Lemma 4.4. *Let I be an upward closed set. Then $\mathcal{M}(I)$ is finite, and $I = \mathcal{U}(\mathcal{M}(I))$.*

Proof: $\mathcal{M}(I)$ is an antichain, and therefore finite by Corollary 4.2. Now let $\mathbf{i} \in I$. Since $(\mathbb{N}_0^m, \leq)$ has no infinite descending chains, there is a minimal element $\mathbf{z} \in I$ with $\mathbf{z} \leq \mathbf{i}$, and therefore $\mathbf{i} \in \mathcal{U}(\mathcal{M}(I))$. Since $\mathcal{M}(I) \subseteq I$, we obtain the inclusion $\mathcal{U}(\mathcal{M}(I)) \subseteq I$ immediately from the fact that I is upward closed. $\square$

Corollary 4.5. *Let $m \in \mathbb{N}$. The set $\mathbb{N}_0^m$ has no infinite ascending sequence $U_1 \subset U_2 \subset U_3 \ldots$ of upward closed subsets.*

Let $U := \bigcup\{U_i \mid i \in \mathbb{N}\}$. The set U is upward closed, and therefore its set of minimal elements $\mathcal{M}(U)$ is finite. Thus, there is a $j \in \mathbb{N}$ such that $\mathcal{M}(U) \subseteq U_j$. Thus $\mathcal{U}(\mathcal{M}(U)) \subseteq \mathcal{U}(U_j)$, and hence $U \subseteq U_j$. $\square$

We will also use the following Theorem.

Theorem 4.6 (cf. [Maclagan, 2001, Theorem 1.2])**.** *Let $m \in \mathbb{N}$, and let $\mathcal{L}$ be the set of upward closed subsets of $\mathbb{N}_0^m$. Then the partially ordered set $(\mathcal{L}, \subseteq)$ has no infinite antichain.*

[1] Deutsche Übersetzung: *Ordnungsfilter*.

Proof: Since the case $m = 1$ is obvious, we assume $m \geq 2$. For every upward closed subset F of $\mathbb{N}_0^m$ we define a mapping $\Phi_F : \mathbb{N}_0^{m-1} \to \mathbb{N}_0 \cup \{\infty\}$ by

$$\Phi_F(\mathbf{a}) := \begin{cases} \min\{c \in \mathbb{N}_0 \,|\, (\mathbf{a}, c) \in F\} & \text{if there is a } c \in \mathbb{N} \text{ with } (\mathbf{a}, c) \in F, \\ \infty & \text{else.} \end{cases}$$

for $\mathbf{a} \in \mathbb{N}_0^{m-1}$. We first observe that for all $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^{m-1}$ with $\mathbf{a} \leq \mathbf{b}$, we have $\Phi_F(\mathbf{a}) \geq \Phi_F(\mathbf{b})$. To show this, let $c := \Phi_F(\mathbf{a})$ and assume $c \neq \infty$. Then $(\mathbf{a}, c) \in F$. Since F is upward closed, we have $(\mathbf{b}, c) \in F$, and therefore $\Phi_F(\mathbf{b}) \leq c = \Phi_F(\mathbf{a})$. Furthermore, for two upward closed subsets F, G of $\mathbb{N}_0^m$, we have $F \subseteq G$ if and only if $\Phi_F(\mathbf{a}) \geq \Phi_G(\mathbf{a})$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^{m-1}$.

Now let $\langle F_i \,|\, i \in \mathbb{N} \rangle$ be an infinite antichain in $\mathcal{L}$. For $i, j \in \mathbb{N}$ with $i < j$ we therefore have $F_i \not\supseteq F_j$. Hence we have an $\mathbf{a}^{(i,j)} \in \mathbb{N}_0^{m-1}$ such that

$$\Phi_{F_i}(\mathbf{a}^{(i,j)}) > \Phi_{F_j}(\mathbf{a}^{(i,j)}).$$

Now for $i, j, k \in \mathbb{N}$ with $i < j < k$, we color the three element subset $\{i, j, k\}$ with $i < j < k$ with one of 2^{m-1} colors. As colors, we take the functions from $\{1, \dots, m-1\}$ to $\{\boldsymbol{\leq}, \boldsymbol{>}\}$. For $l \in \{1, \dots, m-1\}$, let the l-th component of $\mathbf{a}^{(i,j)}$ be denoted by $\mathbf{a}_l^{(i,j)}$. Now we define the color of $\{i, j, k\}$ by

$$C(\{i, j, k\})\,(l) := \begin{cases} \boldsymbol{\leq} & \text{if } \mathbf{a}_l^{(i,j)} \leq \mathbf{a}_l^{(j,k)}, \\ \boldsymbol{>} & \text{if } \mathbf{a}_l^{(i,j)} > \mathbf{a}_l^{(j,k)}. \end{cases}$$

By Ramsey's Theorem [Ramsey, 1929], $\mathbb{N}$ has an infinite subset T such that all 3-element subsets of T have the same color C. We will now show that $C(l) = \boldsymbol{\leq}$ for all $l \in \{1, \dots, m-1\}$.

Seeking a contradiction, we suppose that there is a l such that $C(l) = \boldsymbol{>}$. Let $t_1 \leq t_2 \leq t_3 \dots$ be the elements of T. If $C(l) = \boldsymbol{>}$, we have

$$\mathbf{a}_l^{(t_1,t_2)} > \mathbf{a}_l^{(t_2,t_3)} > \mathbf{a}_l^{(t_3,t_4)} > \cdots,$$

and hence an infinitely descending chain of natural numbers, which is impossible.

Thus, for all $r \in \mathbb{N}$, we have $\mathbf{a}^{(t_r,t_{r+1})} \leq \mathbf{a}^{(t_{r+1},t_{r+2})}$. Now fix $r \in \mathbb{N}$. Then by the choice of $\mathbf{a}^{(t_r,t_{r+1})}$, we have

$$\Phi_{F_{t_r}}(\mathbf{a}^{(t_r,t_{r+1})}) > \Phi_{F_{t_{r+1}}}(\mathbf{a}^{(t_r,t_{r+1})}).$$

Since $\mathbf{a}^{(t_r,t_{r+1})} \leq \mathbf{a}^{(t_{r+1},t_{r+2})}$, we have

$$\Phi_{F_{t_{r+1}}}(\mathbf{a}^{(t_r,t_{r+1})}) \geq \Phi_{F_{t_{r+1}}}(\mathbf{a}^{(t_{r+1},t_{r+2})}).$$

Altogether, the sequence $\langle \Phi_{F_{t_i}}(\mathbf{a}^{(t_i,t_{i+1})}) \,|\, i \in \mathbb{N} \rangle$ is an infinitely descending sequence in $\mathbb{N}_0 \cup \{\infty\}$, which is impossible.

Hence there cannot be an infinite antichain $\langle F_i \,|\, i \in \mathbb{N} \rangle$ of upward closed subsets of $\mathbb{N}_0^m$. $\square$

References

[Dickson, 1913] Dickson, L. E. (1913). Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *American Journal of Mathematics*, 35(4):413–422.

[Maclagan, 2001] Maclagan, D. (2001). Antichains of monomial ideals are finite. *Proc. Amer. Math. Soc.*, 129(6):1609–1615 (electronic).

[Ramsey, 1929] Ramsey, F. P. (1929). On a problem of formal logic. *Proceedings London Mathematical Society (2)*, 30:264–286.