Reelle Algebra

Prof. Dr. Alexander Prestel*

Wintersemester 2007/08

*geTEXt von David Grimm, Tim Netzer, Ute Otterbeck und Sven Wagner

Inhaltsverzeichnis

1 Angeordnete Körper

1.1 Anordnungen und Positivbereiche

Definition 1.1. Eine zweistellige Relation $\leq$ auf einer Menge heißt *partielle Ordnung*, falls für alle Elemente a, b, c der Menge gilt:

(i) $a \leq a$

(ii) $a \leq b$ und $b \leq a \Longrightarrow a = b$

(iii) $a \leq b$ und $b \leq c \Longrightarrow a \leq c$.

Die Ordnung heißt *lineare Ordnung*, falls zusätzlich für alle a, b gilt:

(iv) $a \leq b$ oder $b \leq a$.

Die Mengeninklusion $\subseteq$ ist beispielsweise eine partielle aber nicht lineare Ordnung auf der Potenzmenge einer Menge.

Definition 1.2. $(K, \leq)$ heißt *angeordneter Körper*, falls K Körper und $\leq$ lineare Ordnung von K ist und für alle Elemente $a, b, c \in K$ zusätzlich gilt

(i) $a \leq b \Longrightarrow a + c \leq b + c$

(ii) $0 \leq a, b \Longrightarrow 0 \leq ab$.

Folgerungen 1.3. Ist $(K, \leq)$ angeordneter Körper, so gilt für alle Elemente $a, b, c \in K$:

(0) $a \leq b \Longleftrightarrow 0 \leq b - a$

(i) $0 \leq a^2$:

$$\begin{aligned} &0 \leq a \Longrightarrow 0 \leq a^2 \\ &a \leq 0 \Longrightarrow 0 \leq -a \Longrightarrow 0 \leq (-a)(-a) = a^2 \end{aligned}$$

(ii) $a \leq b, 0 \leq c \Longrightarrow ac \leq bc$:

$$\begin{aligned} a \leq b &\Longrightarrow 0 \leq b - a \\ &\Longrightarrow 0 \leq (b - a)c \\ &\Longrightarrow ac \leq bc \end{aligned}$$

(iii) $0 < a < b \Longrightarrow 0 < \frac{1}{b} < \frac{1}{a}$:

$$\text{für alle } c \text{ gilt: } 0 < c \Longrightarrow 0 < \frac{c}{c^2} = \frac{1}{c}, \text{ also}$$
$$0 < b - a \Longrightarrow 0 < \frac{b-a}{ab} = \frac{1}{a} - \frac{1}{b}$$

(iv) $0 < ab \Longleftrightarrow 0 < \frac{a}{b}$

(v) $0 < n$ für alle $n \in \mathbb{N} \setminus \{0\}$:

Induktion über n:
$n = 1 : 0 < 1^2 = 1$
$n \to n+1 : 0 < n \Longrightarrow 1 = 1 + 0 \leq n + 1$
$\Longrightarrow 0 < 1 \leq n + 1$

Insbesondere hat K die Charakteristik 0.

Beispiele 1.4. (1) $(\mathbb{Q}, \leq), (\mathbb{R}, \leq)$

(2) Betrachte die Einbettung $\varphi_0 \colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{R}, \sqrt{2} \mapsto \sqrt{2}$. Dann definiert

$$\alpha \leq_0 \beta :\Longleftrightarrow \varphi_0(\alpha) \leq \varphi_0(\beta)$$

eine Anordnung auf $\mathbb{Q}(\sqrt{2})$. Analog erhält man eine Anordnung für $\varphi_1 \colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{R}, \sqrt{2} \mapsto -\sqrt{2}$.

(3) $\mathbb{R}(X)$: definiere für $f = a_r X^r + a_{r+1} X^{r+1} + \cdots + a_n X^n \in \mathbb{R}[X]$ mit $a_r \neq 0$:

$$0 < f :\Longleftrightarrow 0 < a_r$$

(d.h. $f > 0$ gdw. der kleinste nichttriviale Koeffizient von f größer 0), anschließend für $f, g \in \mathbb{R}[X]$

$$\begin{aligned} g < f &:\Longleftrightarrow 0 < f - g \\ 0 < \frac{f}{g} &:\Longleftrightarrow 0 < fg \end{aligned}$$

Dies liefert eine Anordnung auf $\mathbb{R}(X)$ mit $0 < \alpha \pm X$ für alle $\alpha \in \mathbb{R}$ mit $0 < \alpha$, d.h. $\pm X < \alpha$. X ist also positiv aber kleiner als alle reellen Zahlen. Insbesondere gilt $n < X^{-1}$ für alle $n \in \mathbb{N}$.

(4) $\mathbb{R}((X))$: Körper der formalen Potenzreihen, d.h.

$$\mathbb{R}((X)) := \left\{ \sum_{i=m}^{\infty} a_i X^i \mid m \in \mathbb{Z}, a_i \in \mathbb{R} \right\}.$$

Die Anordnung wird analog zum vorherigen Beispiel definiert.

Definition 1.5. $(K, \leq)$ heißt *archimedisch angeordnet*, falls es zu jedem $\alpha \in K$ ein $n \in \mathbb{N}$ mit $\alpha \leq n$ gibt.

Satz 1.6 (Hölder). *Jeder archimedisch angeordnete Körper $(K, \leq)$ erlaubt einen ordnungstreuen Monomorphismus in $(\mathbb{R}, \leq)$, d.h. es gibt eine Abbildung $\varrho\colon K \longrightarrow \mathbb{R}$ mit*

(1) ϱ ist Monomorphismus und

(2) $\alpha \leq \beta \Longleftrightarrow \varrho(\alpha) \leq \varrho(\beta)$ für alle $\alpha, \beta \in K$.

Wir benötigen für den Beweis das folgende Lemma:

Lemma 1.7. *Sei $(K, \leq)$ archimedisch. Dann liegt $\mathbb{Q}$ dicht in $(K, \leq)$, d.h. zu $a < b$ in K gibt es ein $r \in \mathbb{Q}$ mit $a < r < b$.*

Beweis. Sei $a < b$, d.h. $b - a > 0$. Also gilt $0 < \frac{1}{b-a} < m$ für ein $m \in \mathbb{N}$, da K archimedisch. Daraus folgt $1 < m(b-a)$, also $ma < mb - 1$. Wähle nun ein $n \in \mathbb{Z}$ minimal mit $mb \leq n + 1$. Damit gilt

$$ma < mb - 1 \leq n < mb,$$

und somit

$$a < \frac{n}{m} < b.$$

□

Sei wieder $(K, \leq)$ ein angeordneter Körper und $O, U \subseteq K$. Wir schreiben $U \leq O$ für die Aussage, dass $u \leq o$ gilt für alle $u \in U, o \in O$.

Definition 1.8. $(K, \leq)$ heißt *schnittvollständig*, falls für alle $U, O \subseteq K$ mit $U, O \neq \emptyset$ und $U \leq O$ ein α aus K mit $U \leq \{\alpha\} \leq O$ existiert.
$U \leq O$ heißt *Dedekindschnitt*, falls $U, O \neq \emptyset$ und $U \cup O = K$.

Lemma 1.9. *Jeder schnittvollständige Körper $(K, \leq)$ ist archimedisch.*

Beweis. Annahme: Es gibt ein $\alpha_0 \in K$ mit $n \leq \alpha_0$ für alle $n \in \mathbb{N}$. Setze $U := \mathbb{N}$ und $O := \{\alpha \in K \mid \alpha \geq u \text{ für alle } u \in U\} \ni \alpha_0$.
Sei $U \leq \beta \leq O$ für ein $\beta \in K$. Dann gilt $\mathbb{N} \leq \beta$, also auch $\mathbb{N} \leq \beta - 1$, und somit $\beta - 1 \in O$, d.h. $\beta \leq \beta - 1$, Widerspruch. □

Beweis. (zum Satz von Hölder) Betrachte zu $a \in K$ die Mengen

$$U_a := \{s \in \mathbb{Q} \mid s < a\} \text{ und } O_a := \{r \in \mathbb{Q} \mid a \leq r\}.$$

Es gilt $U_a \leq O_a, U_a \cup O_a = \mathbb{Q}, U_a \cap O_a = \emptyset$ und $U_a, O_a \neq \emptyset$ (da K archimedisch). Da $\mathbb{R}$ schnittvollständig ist, gibt es ein $x \in \mathbb{R}$ mit $U_a \leq x \leq O_a$. Dieses x ist eindeutig bestimmt, denn sei $U_a \leq x' \leq O_a$ und etwa $x < x'$, so wähle $t \in \mathbb{Q}$ mit $x < t < x'$. Dann gilt

$$t < x' \Longrightarrow t \in U_a$$
$$x < t \Longrightarrow t \in O_a,$$

Widerspruch.
Setze nun $\varrho(a) := x$. Dann ist ϱ (nach Aufgabe 1.2) eine ordnungstreue Körpereinbettung (hierfür wird Lemma 1.7 benötigt). □

Korollar 1.10. $(\mathbb{R}, \leq)$ *ist bis auf Isomorphie der einzige schnittvollständige Körper.*

Beweis. Sei $(K, \leq)$ schnittvollständig. Dann ist $(K, \leq)$ nach Lemma 1.9 archimedisch und lässt sich also ordnungstreu in $(\mathbb{R}, \leq)$ einbetten. Es ist somit nur noch die Surjektivität der Abbildung aus dem vorherigen Beweis zu zeigen.
Zu $x \in \mathbb{R}$ definiere die Mengen U_x und O_x wie oben. In K gibt es dann ein Element a mit $U_x \leq \{a\} \leq O_x$, dieses ist aber offensichtlich Urbild von x unter der oben definierten Abbildung. □

Definition 1.11. Sei $T \subseteq K$. T heißt *Präpositivbereich* oder *Präordnung*, falls $T + T \subseteq T,\ T \cdot T \subseteq T,\ K^2 \subseteq T$ und $-1 \notin T$ gilt.
T heißt *Positivbereich*, falls zusätzlich $T \cup -T = K$ gilt.

Beachte: Ist T ein Positivbereich, so folgt $K^2 \subseteq T$ schon aus den anderen Axiomen:

$$a \in T \Longrightarrow a^2 = aa \in T$$
$$-a \in T \Longrightarrow a^2 = (-a)(-a) \in T.$$

Beispiel 1.12. Ist $\leq$ eine Anordnung auf K, so ist

$$P_{\leq} := \{x \in K \mid 0 \leq x\}$$

ein Positivbereich.

Lemma 1.13. *Es sei $P \subseteq K$ ein Positivbereich. Dann definiert*

$$a \leq_P b :\Longleftrightarrow b - a \in P$$

eine Anordnung $\leq_P$ auf K.

Beweis.
- $a \leq a$ wegen $a - a = 0 = 0^2 \in P$.
- $a \leq b, b \leq c \Longrightarrow a \leq c$ wegen $P + P \subseteq P$.
- $a \leq b, b \leq a \Longrightarrow a = b$ wegen $P \cap -P = \{0\}$ (gäbe es $0 \neq x \in P \cap -P$, so wäre $-1 = x(-x)\frac{1}{x^2} \in P$, Widerspruch).
- $a \leq b$ oder $b \leq a$ wegen $P \cup -P = K$.
- $a \leq b \Longrightarrow a + c \leq b + c$ trivial.
- $0 \leq a, 0 \leq b \Longrightarrow 0 \leq ab$ wegen $P \cdot P \subseteq P$.

□

Bemerkung 1.14. Es gilt

$$\begin{aligned} P \ &\rightsquigarrow \leq_P \rightsquigarrow \ P_{\leq_P} \ = \ P \\ \leq \ &\rightsquigarrow \ P_{\leq} \ \rightsquigarrow \leq_{P_{\leq}} = \leq, \end{aligned}$$

also entsprechen sich umkehrbar eindeutig:

$$\{\text{Anordnungen auf } K\} \longleftrightarrow \{\text{Positivbereiche von } K\}.$$

Lemma 1.15. *Sei T ein Präpositivbereich von K und $x \in K \setminus T$. Dann ist $T - xT =: T'$ ein Präpositivbereich.*

Beweis. Es gilt offensichtlich $K^2 \subseteq T - xT$ sowie $(T - xT) + (T - xT) \subseteq (T - xT)$. Weiter gilt $(T - xT)(T - xT) \subseteq T - xT + x^2T \subseteq T - xT$.
Falls $-1 = t_1 - xt_2$ für gewisse $t_1, t_2 \in T$, so ist $x = (1 + t_1)\frac{t_2}{t_2^2} \in T$, Widerspruch. □

Satz 1.16. *Sei T Präpositivbereich. Dann gilt*

$$T = \bigcap_{T \subseteq P} P \quad (P \text{ Positivbereich}).$$

Beweis. " $\subseteq$ " : klar.
" $\supseteq$ " : Sei $x \in \bigcap_{T\subseteq P} P$ und $x \notin T$. Dann ist $T' := T - xT$ nach Lemma 1.15 ein Präpositivbereich und $-x \in T'$. Wähle mit Zorns Lemma einen maximalen Präpositivbereich P über T'. Da P maximal ist, folgt $y \in P$ oder $-y \in P$ für alle $y \in K$, wiederum mit Lemma 1.15. Damit ist P aber ein Positivbereich. Da $-x \in P$ und $T \subseteq P$, also auch $x \in P$, folgt $x = 0$, Widerspruch zu $x \notin T$. □

Wir betrachten nun

$$\sum K^2 := \left\{ \sum_{i=1}^{n} a_i^2 \mid n \in \mathbb{N}, a_i \in K \right\}.$$

Offensichtlich gilt $\sum K^2 + \sum K^2 \subseteq \sum K^2$ und $K^2 \subseteq \sum K^2$.

Lemma 1.17. *Ein Körper K besitzt genau dann eine Anordnung, wenn $-1 \notin \sum K^2$.*

Beweis. " $\Rightarrow$ " : klar, da $0 \leq \sum a_i^2$.
" $\Leftarrow$ " : $-1 \notin \sum K^2 \Longrightarrow T = \sum K^2$ ist Präordnung. Sei $P \supseteq T$ maximale Präordnung, dann ist $\leq_P$ eine Anordnung auf K. □

Definition 1.18. K heißt *reeller Körper*, falls $-1 \notin \sum K^2$.

Beachte: K reell $\Longrightarrow \sum K^2 \subseteq T$ für alle Präordnungen T.

Mit Lemma 1.17 und Satz 1.6 erhalten wir für einen Körper K:

a) K besitzt eine Anordnung $\iff$ K ist reell.

b) K besitzt eine archimedische Anordnung $\iff$ K ist ordnungstreu in $\mathbb{R}$ einbettbar.

1.2 Fortsetzungen von Anordnungen

Sei L/K eine Körpererweiterung, $\leq_1$ eine Anordnung auf K und $\leq_2$ eine Anordnung auf L. Wir sagen dass $\leq_2$ die Anordnung $\leq_1$ fortsetzt, falls für alle $a, b \in K$ gilt $a \leq_1 b \iff a \leq_2 b$. Dies ist äquivalent zu $P_2 \cap K = P_1$, wobei P_i der zu $\leq_i$ gehörende Positivbereich ist.
Notation: $(K, \leq_1) \subseteq (L, \leq_2)$ oder $(K, P_1) \subseteq (L, P_2)$.

Lemma 1.19. *Ein Positivbereich P von K kann genau dann auf L fortgesetzt werden, wenn die Menge*

$$T_L(P) := \left\{ \sum_{i=1}^{n} p_i \beta_i^2 \mid n \in \mathbb{N}, p_i \in P, \beta_i \in L \right\}$$

eine Präordnung von L ist.

Beweis. " $\Rightarrow$ " : Sei $(K, P) \subseteq (L, P')$. Dann gilt $T_L(P) \subseteq P'$, also $-1 \notin T_L(P)$. Damit ist $T_L(P)$ aber eine Präordnung, da die restlichen Bedingungen offensichtlich immer erfüllt sind.
" $\Leftarrow$ " : Sei $P' \supseteq T_L(P)$ ein maximaler Präpositivbereich und damit ein Positivbereich von L. Dann gilt $P \subseteq P'' := P' \cap K$. Daraus folgt $P = P''$ mit der folgenden Behauptung: □

Behauptung 1.20. *Sind $P \subseteq P'$ Positivbereiche von K, so gilt $P = P'$.*

Beweis. Sei $x \in P', x \notin P$, dann folgt $-x \in P \subseteq P'$, also $x = 0$, Widerspruch zu $x \notin P$. □

Satz 1.21. *Sei $L = K(\sqrt{a})$ für ein $a \in K \setminus K^2$. Sei P Positivbereich von K. Genau dann hat P eine Fortsetzung auf L, wenn $a \in P$.*

Beweis. " $\Rightarrow$ " : Sei $(K, P) \subseteq (L, P')$. Dann gilt $a = (\sqrt{a})^2 \in P' \cap K = P$.
" $\Leftarrow$ " : Sei $a \in P$. Annahme: $-1 \in T_L(P)$, d.h.

$$-1 = \sum a_i (x_i + y_i \sqrt{a})^2$$

für gewisse $a_i \in P, x_i, y_i \in K$. Dann erhält man durch Koeffizientenvergleich

$$-1 = \sum (a_i x_i^2 + a_i a y_i^2) \in P,$$

Widerspruch. Somit ist $T_L(P)$ eine Präordnung und mit Lemma 1.19 läßt sich P fortsetzen. □

Satz 1.22. *Sei $[L : K] = 2n+1$ ungerade. Dann läßt sich jeder Positivbereich P von K auf L fortsetzen.*

Beweis. Annahme: Es gibt einen angeordneten Körper (K, P) und eine Erweiterung von K von ungeradem Grad, so dass sich P nicht auf den Oberkörper fortsetzen lässt. Wähle unter diesen Erweiterungen eine Erweiterung L/K von minimalem Grad $2n + 1$. Es gilt mit dem Satz vom primitiven Element

$$L = K(\alpha) = K[X]/(f)$$

für ein $\alpha \in L$ und sein Minimalpolynom $f = \mathrm{Irr}(\alpha, K)$.
Nach Lemma 1.19 gilt nun

$$-1 = \sum_{i=1}^{m} a_i \gamma_i^2$$

für ein $m \in \mathbb{N}$ und gewisse $a_i \in P, \gamma_i \in L$. Das bedeutet aber, dass $f_1, \ldots, f_m \in K[X]$ existieren mit

$$-1 \equiv \sum_{i=1}^{m} a_i f_i(X)^2 \mod (f).$$

Dabei können die f_i mit $\deg f_i \leq 2n$ gewählt werden. Also gibt es ein $h \in K[X]$ mit

$$1 + \sum_{i=1}^{m} a_i f_i(X)^2 = f(X)h(X).$$

Dabei ist wegen $a_i \in P$ für $i = 1, \ldots, m$ der Grad auf der linken Seite gerade (denn die Monome vom höchsten Grad können sich nicht gegenseitig aufheben), ausserdem kleiner gleich $4n$. Also muss h von ungeradem Grad kleiner gleich $2n - 1$ sein (da $\deg f = 2n + 1$, ungerade).
Wähle also einen irreduziblen Faktor h_1 von h von ungeradem Grad und eine Nullstelle β von h_1. Dann ist $[K(\beta) : K]$ ungerade und echt kleiner als $[L : K]$. Ausserdem lässt sich P nicht auf $K(\beta)$ fortsetzen, denn Einsetzen von β in die obere Gleichung liefert $-1 = \sum_{i=1}^{m} a_i \varrho_i^2$ für $\varrho_i = f_i(\beta) \in K(\beta)$. Dies ist ein Widerspruch zur Minimalität von $[L : K]$. □

Satz 1.23. *Jeder Positivbereich P eines Körpers K läßt sich auf $K(X)$ fortsetzen.*

Beweis. Angenommen es gibt $a_1, \ldots, a_m \in P$ und $f_1, \ldots, f_m \in K(X)$ mit

$$-1 = \sum_{i=1}^{m} a_i f_i(X)^2.$$

Schreibe $f_i = \frac{g_i}{h}$ mit Polynomen $g_i, h \in K[X]$, wobei kein irreduzibler Faktor von h alle g_i teile. Also gilt

$$-h(X)^2 = \sum_{i=1}^{m} a_i g_i(X)^2.$$

Einsetzen von 0 liefert dann einen Widerspruch, da entweder die linke Seite negativ ist, die rechte aber nicht, oder die linke Seite 0, die rechte aber echt positiv ist (denn mindestens eines der g_i hat dann 0 nicht als Nullstelle).
Also folgt die Aussage mit Lemma 1.19. □

1.3 Reell abgeschlossene Körper

Definition 1.24. Ein angeordneter Körper $(K, \leq)$ heißt *maximal angeordnet*, falls sich die Anordnung $\leq$ auf keine echte algebraische Erweiterung von K fortsetzen läßt.

Lemma 1.25. *Ist $(K, \leq)$ maximal angeordnet, so ist jedes nichtnegative Element in K ein Quadrat. Insbesondere ist $\leq$ die einzige Anordnung auf K.*

Beweis. Sei $a \in K$ mit $a \geq 0$. Wäre nun $a \notin K^2$, so ließe sich die Anordnung nach Satz 1.21 auf die echte algebraische Erweiterung $K(\sqrt{a})$ fortsetzen, Widerspruch.
Insbesondere ist K^2 nach Behauptung 1.20 die einzige Anordnung von K, denn sie ist in allen anderen möglichen enthalten. □

Definition 1.26. Ein Körper heißt *reell abgeschlossen*, wenn er reell ist, aber keine echte reelle algebraische Erweiterung besitzt.

Lemma 1.27. *Für einen Körper K sind die folgenden Aussagen äquivalent:*

(i) K ist reell abgeschlossen

(ii) K besitzt genau eine Anordnung $\leq$, und bezüglich dieser ist er maximal angeordnet

Beweis. " $\Rightarrow$ " : Sei $\leq$ eine Anordnung von K. Dann ist $(K, \leq)$ maximal angeordnet und nach Lemma 1.25 ist $\leq$ die einzige Anordnung auf K.
" $\Leftarrow$ " : Hätte K eine echte reelle algebraische Erweiterung L, so würde jede Anordnung auf L natürlich die einzige Anordnung auf K fortsetzen. Das widerspricht der Voraussetzung. □

Satz 1.28 (Artin & Schreier, 1926). *Für einen Körper K sind äquivalent:*

(i) *K ist reell abgeschlossen*

(ii) *K^2 ist Positivbereich von K und jedes Polynom $p \in K[X]$ von ungeradem Grad hat eine Nullstelle in K*

(iii) *$K \neq K(\sqrt{-1})$ und $K(\sqrt{-1})$ ist algebraisch abgeschlossen*

Beweis. "$(i) \Rightarrow (ii)$" : Mit Lemma 1.27 und Lemma 1.25 folgt, dass K^2 Positivbereich von K ist.
Sei nun $p \in K[X]$ von ungeradem Grad und o.B.d.A. irreduzibel (sonst betrachte einen irreduziblen Faktor von p von ungeradem Grad). Dann ist $L := K[X]/(p)$ eine algebraische Erweiterung von ungeradem Grad von K, auf die sich nach Satz 1.22 die Anordnung von K fortsetzen läßt. Da K reell abgeschlossen ist folgt $L = K$, also hat p eine Nullstelle in K.
"$(ii) \Rightarrow (iii)$" : Es gilt $\sqrt{-1} \notin K$, da sonst $-1 = \sqrt{-1}^2 \in K^2$. Also ist $K \neq K(\sqrt{-1})$.
Sei nun L eine algebraische Erweiterung von $K(\sqrt{-1})$. Wir zeigen $L = K(\sqrt{-1})$, daraus folgt die algebraische Abgeschlossenheit.
Sei o.B.d.A L/K eine Galoiserweiterung (sonst ersetze L durch den Zerfällungskörper des Minimalpolynoms über K eines primitiven Elements der Erweiterung L/K).
Sei $G = \mathrm{Gal}(L/K)$ die Galoisgruppe der Erweiterung und schreibe $|G| = 2^e m$ mit $e, m \in \mathbb{N}$ und $2 \nmid m$. Dabei ist $e > 0$, da $2 \mid [L : K]$. Also können wir eine 2-Sylowuntergruppe H von G wählen und $F = \mathrm{Fix}\, H$, den Fixkörper zu H, betrachten:

$$\begin{array}{cc} L & \{\mathrm{id}\} \\ 2^e \mid & \mid 2^e \\ F & H \\ m \mid & \mid m \\ K & G \end{array}$$

Es ist $[F : K] = |G : H| = m$ ungerade, somit folgt aus (ii) $F = K$, also $m = 1$.

Also ist $[L : K(\sqrt{-1})] = \frac{1}{2}[L : K] = 2^{e-1}$. Wäre nun $e > 1$, so könnten wir eine Untergruppe H_1 von $G_1 = \mathrm{Gal}(L/K(\sqrt{-1}))$ vom Index 2 wählen und erhielten als deren Fixkörper eine quadratische Erweiterung F_1 von $K(\sqrt{-1})$:

$$\begin{array}{ccc} L & & \{\mathrm{id}\} \\ {\scriptstyle 2^{e-2}}\,| & & |\,{\scriptstyle 2^{e-2}} \\ F_1 & & H_1 \\ {\scriptstyle 2}\,| & & |\,{\scriptstyle 2} \\ K(\sqrt{-1}) & & G_1 \\ {\scriptstyle 2}\,| & & |\,{\scriptstyle 2} \\ K & & G \end{array}$$

Dies widerspricht aber der folgenden Behauptung:

Behauptung: Ist K^2 ein Positivbereich von K, so ist $K(\sqrt{-1})$ quadratisch abgeschlossen, d.h. jedes Element in $K(\sqrt{-1})$ ist ein Quadrat.

Beweis: Betrachte $a + b\sqrt{-1}$ mit $a, b \in K$. Da $a^2 + b^2 \in K^2$, gibt es $\sqrt{a^2 + b^2} \in K$.

Es gilt $|a| \leq |\sqrt{a^2 + b^2}|$, wobei der Betrag wie üblich definiert ist, d.h.

$$|a| := \begin{cases} a, & \text{falls } a \geq 0; \\ -a, & \text{falls } a \leq 0. \end{cases}$$

Also folgt $|\sqrt{a^2 + b^2}| \pm a \in K^2$. Setze

$$x := \sqrt{\frac{a + |\sqrt{a^2 + b^2}|}{2}} \text{ und } y := \sqrt{\frac{-a + |\sqrt{a^2 + b^2}|}{2}}$$

und rechne nach, dass $(x + y\sqrt{-1})^2 = a + b\sqrt{-1}$ gilt. $\square$

"$(iii) \Rightarrow (i)$" : Wir zeigen $K^2 + K^2 \subseteq K^2$. Dann folgt aus der Voraussetzung $-1 \notin \sum K^2$, also ist K reell. Da die einzige echte algebraische Erweiterung von K nicht reell ist ($-1 \in K(\sqrt{-1})^2$), folgt die Behauptung.

Seien also $a, b \in K$ beliebig und dazu $x, y \in K$ mit $a + b\sqrt{-1} = (x + y\sqrt{-1})^2$ ($K(\sqrt{-1})$ ist algebraisch abgeschlossen). Aus Koeffizientenvergleich folgt $a = x^2 - y^2$ und $b = 2xy$.

Also ist

$$a^2 + b^2 = x^4 - 2x^2y^2 + y^4 + 4x^2y^2 = (x^2 + y^2)^2 \in K^2.$$

□

Bemerkung 1.29. Für $K = \mathbb{R}$ ist (ii) aus dem Satz von Artin & Schreier erfüllt, wie man in der Analysis leicht zeigt. Also ist $\mathbb{R}$ wegen $(ii) \Rightarrow (i)$ reell abgeschlossen. Ausserdem folgt wegen $(ii) \Rightarrow (iii)$, dass $\mathbb{C}$ algebraisch abgeschlossen ist.
So wie $\mathbb{C}$ der 'Prototyp' aller algebraisch abgeschlossenen Körper ist, ist $\mathbb{R}$ der Prototyp der reell abgeschlossenen Körper.

Satz 1.30. *Sei K reell abgeschlossen. Dann gilt für $f \in K[X]$:*

(a) f *irreduzibel, normiert* $\Longrightarrow$ $f = X - a$ *oder* $f = (X - a)^2 + b^2$ *mit* $b \neq 0$

(b) Sei $a < b$ *und* $f(a) < 0 < f(b)$*, dann existiert ein* $c \in (a, b)$ *mit* $f(c) = 0$

Beweis. (a): Ist f irreduzibel, so folgt $\deg f = 1$ oder $\deg f = 2$ aus Satz 1.28(iii) (denn ein irreduzibles Polynom vom Grad ≥ 3 ergäbe eine algebraische Erweiterung von K von ebendiesem Grad; K hat aber bis auf Isomorphie nur eine algebraische Erweiterung, und die ist quadratisch).
Jedes normierte Polynom vom Grad 1 hat aber über K die Gestalt $X - a$ für ein $a \in K$.
Hat f den Grad 2, so lässt sich f darstellen als $f = X^2 - 2aX + c = (X - a)^2 + (c - a^2)$ mit geeigneten $a, c \in K$. Dann folgt aber $c - a^2 > 0$ aus der Irreduzibilität von f (wäre $c - a^2 \leq 0$, so wäre $-(c - a^2)$ in K ein Quadrat und f hätte also eine Nullstelle). Also ist $c - a^2 \in K^2 \setminus \{0\}$.
(b): Zerlege f in irreduzible Faktoren:

$$f = c \prod_{i=1}^{n} (X - a_i) \prod_{j=1}^{m} ((X - d_j)^2 + b_j^2), \qquad \text{alle } b_j \neq 0.$$

Nun muss aber der Vorzeichenwechsel von f zwischen a und b von einem der auftretenden Linearfaktoren kommen, d.h. mindestens einer der Linearfaktoren muss bei a und b ebenfalls unterschiedliche Vorzeichen haben. Denn

das Vorzeichen von f an einer Stelle berechnet sich als das Produkt der Vorzeichen der Linearfaktoren an dieser Stelle und dem Vorzeichen von c (alle irreduziblen Faktoren vom Grad 2 nehmen nur positive Werte an).
Ein Vorzeichenwechsel eines Linearfaktors $(X - a_i)$ zwischen a und b bedeutet aber dass a_i zwischen a und b liegt. Dieses a_i ist aber eine Nullstelle von f. □

Definition 1.31. Sei $(K, \leq)$ ein angeordneter Körper. Ein angeordneter Körper $(L, \leq)$ heißt *reeller Abschluss* von $(K, \leq)$, falls $(K, \leq) \subseteq (L, \leq)$ eine algebraische Erweiterung angeordneter Körper und L reell abgeschlossen ist.

Satz 1.32. *Jeder angeordnete Körper besitzt einen reellen Abschluss.*

Beweis. Sei (K, P) angeordneter Körper. Betrachte die Menge aller Tupel (L, Q), wobei L eine algebraische Erweiterung von K und Q eine Fortsetzung von P auf L sei. Die Menge lässt sich partiell ordnen durch

$$(L, Q) \subseteq (L', Q') :\Longleftrightarrow L \subseteq L' \text{ und } Q' \cap L = Q.$$

Mit dieser partiellen Ordnung erfüllt die Menge aber die Voraussetzungen des Zorn'schen Lemmas und wir können ein maximales solches Tupel $(\hat{L}, \hat{Q})$ wählen. Dann ist $(\hat{L}, \hat{Q})$ aber offensichtlich maximal angeordnet und also mit Lemma 1.27 reell abgeschlossen. Da $\hat{L}/K$ algebraisch ist, ist $(\hat{L}, \hat{Q})$ ein reeller Abschluss von (K, P). □

Definition 1.33. $\varphi\colon (K_1, \leq_1) \longrightarrow (K_2, \leq_2)$ heißt *Ordnungseinbettung*, falls $\varphi\colon K_1 \longrightarrow K_2$ ein Monomorphismus ist und $\varphi(a) \leq_2 \varphi(b)$ für alle $a, b \in K_1$ mit $a \leq_1 b$ gilt. Analog definiert man *Ordnungsisomorphismus*.

Wir wollen nun den folgenden Satz zeigen:

Satz 1.34 (Artin & Schreier). *Zwei reelle Abschlüsse eines angeordneten Körpers $(K, \leq)$ sind immer ordnungsisomorph über K.*

Dann ist es auch sinnvoll, die folgende Bezeichnung zu verwenden:

Bezeichnung. Wir schreiben $\overline{(K, \leq)}$ für *den* reellen Abschluss eines angeordneten Körpers $(K, \leq)$.

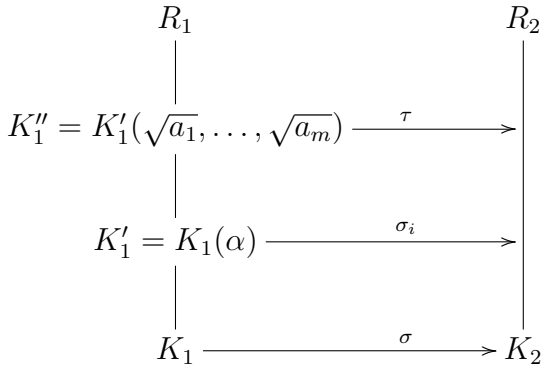
Für den Beweis von Satz 1.34 brauchen wir zunächst den folgenden Satz, den wir erst im nächsten Kapitel beweisen werden:

Satz 1.35 (Übertragungssatz). *Sind (R_1, R_1^2), (R_2, R_2^2) zwei reell abgeschlossene Oberkörper von (K, P), so hat jedes Polynom $p \in K[X]$, welches in R_1 eine Nullstelle hat, auch eine Nullstelle in R_2.*

Mit diesem Satz zeigen wir nun das folgende Lemma:

Lemma 1.36. *Sei $\sigma\colon (K_1, P_1) \longrightarrow (K_2, P_2)$ ein Ordnungsisomorphismus, seien (R_i, R_i^2) reelle Abschlüsse von (K_i, P_i) (für $i = 1, 2$), und sei $(K_1', P_1') \subseteq (R_1, R_1^2)$ eine endliche Erweiterung von (K_1, P_1). Dann lässt sich σ fortsetzen zu einer Ordnungseinbettung $\sigma'\colon (K_1', P_1') \longrightarrow (R_2, R_2^2)$.*

Beweis. Wähle mit dem Satz vom primitiven Element ein $\alpha \in R_1$ mit $K_1' = K_1(\alpha)$. Sei $p = \operatorname{Irr}(\alpha, K_1)$ das Minimalpolynom von α über K_1 und $\sigma(p)$ das Polynom über K_2, welches man durch Anwendung von σ auf die Koeffizienten von p erhält. Nach dem Übertragungssatz muss $\sigma(p)$ eine Nullstelle in R_2 haben (identifiziere die ordnungsisomorphen Körper (K_1, P_1) und (K_2, P_2)).
Also gibt es eine Einbettung von K_1' in R_2, welche σ fortsetzt. Es bleibt zu zeigen, dass es auch eine solche Einbettung gibt, die ordnungserhaltend ist.



Seien $\sigma_1, \ldots, \sigma_m$ alle Einbettungen von K_1' in R_2, welche σ fortsetzen (es gibt höchstens $\deg p$ viele).
Annahme: Keines dieser σ_i ist ordnungserhaltend. Dann gibt es Elemente $a_i \in K_1' \cap R_1^2$ mit $\sigma_i(a_i) \notin R_2^2$ für $i = 1, \ldots, m$.
Betrachte $K_1'' := K_1'(\sqrt{a_1}, \ldots, \sqrt{a_m}) \subseteq R_1$ und wähle eine Einbettung τ von K_1'' in R_2, welche σ fortsetzt (die Existenz eines solchen τ haben wir gerade schon gezeigt).
$\tau|_{K_1'}$ ist also eine Einbettung von K_1' in R_2, welche σ fortsetzt, also $\tau|_{K_1'} = \sigma_j$ für ein j.

Damit folgt aber

$$\sigma_j(a_j) = \tau(a_j) = \tau((\sqrt{a_j})^2) = (\tau(\sqrt{a_j}))^2 \in R_2^2,$$

Widerspruch. □

Nun können wir die Eindeutigkeit des reellen Abschlusses beweisen.

Beweis. (zu Satz 1.34) Seien (R_1, R_1^2) und (R_2, R_2^2) zwei reelle Abschlüsse des angeordneten Körpers (K, P).
Betrachte die Menge M aller Tripel $((K_1, P_1), \sigma, (K_2, P_2))$, wobei (K_i, P_i) ein Zwischenkörper von (K, P) und (R_i, R_i^2) sei und σ ein Ordnungsisomorphismus von (K_1, P_1) und (K_2, P_2), welcher die Identität auf K fortsetzt.

$$\begin{array}{ccc} (R_1, R_1^2) & & (R_2, R_2^2) \\ | & & | \\ (K_1, P_1) & \xrightarrow{\sigma} & (K_2, P_2) \\ | & & | \\ (K, P) & \xrightarrow{\mathrm{id}} & (K, P) \end{array}$$

Die Menge M lässt sich partiell ordnen durch

$$((K_1, P_1), \sigma, (K_2, P_2)) \subseteq ((K_1', P_1'), \sigma', (K_2', P_2'))$$
$$gdw.$$
$$(K_1, P_1) \subseteq (K_1', P_1'),\ (K_2, P_2) \subseteq (K_2', P_2') \text{ und } \sigma'|_{K_1} = \sigma.$$

Mit dieser partiellen Ordnung erfüllt M die Voraussetzungen des Zorn'schen Lemmas und wir können ein maximales solches Tripel $((K_1, P_1), \sigma, (K_2, P_2))$ aus M wählen.
Wäre nun etwa $K_1 \neq R_1$, so könnten wir ein $\alpha \in R_1 \setminus K_1$ wählen und nach Lemma 1.36 σ auf die echte Erweiterung $K_1(\alpha)$ von K_1 fortsetzen, Widerspruch.
Falls $K_2 \neq R_2$, wende analog Lemma 1.36 auf σ^{-1} an. □

Korollar 1.37. *Sei (R, R^2) reeller Abschluss von (K, P) und seien K_1, K_2 Zwischenkörper mit der von (R, R^2) induzierten Anordnung. Weiter sei $\sigma\colon K_1 \longrightarrow K_2$ ein ordnungstreuer Isomorphismus über K. Dann gilt $K_1 = K_2$ und $\sigma = \mathrm{id}$. Insbesondere gilt* $\mathrm{Aut}(R/K) = \{\mathrm{id}\}$.

Beweis. Der Beweis des letzten Satzes hat gezeigt, dass wir σ zu einem Ordnungsautomorphismus $\varrho\colon R \longrightarrow R$ fortsetzen können.
Sei nun $\alpha \in R$ und $f = \mathrm{Irr}(\alpha, K)$. Dann ist $\varrho(\alpha)$ wieder Nullstelle von f ($0 = \varrho(0) = \varrho(f(\alpha)) = f(\varrho(\alpha))$; beachte $\varrho|_K = \mathrm{id}$).
Dies gilt für alle Nullstellen von f in R, d.h. ϱ permutiert die Nullstellen von f in R. Da ϱ aber ordnungserhaltend ist, folgt $\varrho(\alpha) = \alpha$, also $\varrho = \mathrm{id}$ (die Reihenfolge der Nullstelle bezüglich der Anordnung wird durch ϱ nicht verändert). □

Bemerkung 1.38. Jeder Monomorphismus $\varrho\colon R \longrightarrow R$ eines reell abgeschlossenen Körpers R ist ordnungstreu: falls $\alpha \geq 0$, so ist $\alpha = \beta^2$ für ein $\beta \in R$. Also ist $\varrho(\alpha) = \varrho(\beta^2) = \varrho(\beta)^2 \geq 0$.

Korollar 1.39. *Sei (R, R^2) reeller Abschluss von (K, P) und sei $\alpha \in R$ sowie $f = \mathrm{Irr}(\alpha, K)$. Dann ist die Anzahl der verschiedenen Fortsetzungen von P auf $K(\alpha)$ gleich der Anzahl der Nullstellen von f in R.*

Beweis. Die Anzahl der Nullstellen von f in R ist gleich der Anzahl der verschiedenen K-Einbettungen von $K(\alpha)$ in R. Es gilt nun:

(a) Jede K-Einbettung $\sigma\colon K(\alpha) \longrightarrow R$ liefert einen Positivbereich P_σ auf $K(\alpha)$, der P fortsetzt:

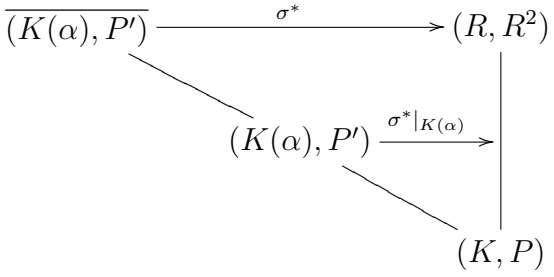
$$\beta \in P_\sigma :\Longleftrightarrow \sigma(\beta) \in R^2.$$

(b) Zwei verschiedene K-Einbettungen liefern dabei unterschiedliche Positivbereiche. Denn ist $P_{\sigma_1} = P_{\sigma_2}$, so ist

$$\sigma_2 \circ \sigma_1^{-1}\colon \sigma_1(K(\alpha)) \longrightarrow \sigma_2(K(\alpha))$$

ein ordnungstreuer Isomorphismus über K. Mit Korollar 1.37 folgt $\sigma_2 \circ \sigma_1^{-1} = \mathrm{id}$, also $\sigma_1 = \sigma_2$.

(c) Jeder Positivbereich auf $K(\alpha)$ der P fortsetzt kommt von einer Einbettung:



Sei P' eine Fortsetzung von P auf $K(\alpha)$. Dann ist der reelle Abschluss $\overline{(K(\alpha), P')}$ auch reeller Abschluss von (K, P), also erhalten wir nach Satz 1.34 einen Ordnungsisomorphismus

$$\sigma^* \colon \overline{(K(\alpha), P')} \longrightarrow (R, R^2)$$

über K. Dann ist $\sigma^*|_{K(\alpha)}$ aber eine K-Einbettung, welche P' als Positivbereich liefert (vgl. (a)).

□

Lemma 1.40. *Sei R reell abgeschlossen und K in R relativ algebraisch abgeschlossener Teilkörper. Dann ist auch K reell abgeschlossen.*

Beweis. $P = R^2 \cap K$ ist Positivbereich auf K. Es gilt nun:

(i) Sei $a \in P$. Dann gilt $a = \beta^2$ für ein $\beta \in R$. Also hat das Polynom $X^2 - a \in K[X]$ in R die Nullstelle β. Da K in R relativ algebraisch abgeschlossen ist, folgt $\beta \in K$. Also ist $P = K^2$.

(ii) Sei $p \in K[X]$ von ungeradem Grad. Dann hat p eine Nullstelle $\beta \in R$, da R reell abgeschlossen ist. Da K in R relativ algebraisch abgeschlossen ist, folgt wiederum $\beta \in R$.

Nach Satz 1.28 ist K also reell abgeschlossen. □

2 Semialgebraische Mengen

2.1 Allgemeines

Sei R ein reell abgeschlossener Körper, R^2 sein (einziger) Positivbereich, $A \subseteq R$ ein Teilring.

Definition 2.1. $S \subseteq R^n$ heißt *semialgebraisch* über A, falls S eine endliche boolsche Kombination (Durchschnitt, Vereinigung,Komplement) von Mengen der Gestalt

$$U(f) = \{a \in R^n \mid f(a) > 0\}$$

mit $f \in A[X] = A[X_1, \ldots, X_n]$ ist.

Beachte: Der kleinste Teilring ist $\mathbb{Z}$.

Definition 2.2. Sei K beliebiger Körper, $A \subseteq K$ Teilring. Dann heißt $S \subseteq K^n$ *algebraisch* über A, falls

$$S = \{a \in K^n \mid f_1(a) = 0, \ldots, f_r(a) = 0\}$$

für gewisse $f_1, \ldots, f_r \in A[X]$ ist.

Bemerkung 2.3. Auch die Vereinigung zweier algebraischer Mengen ist algebraisch, da
$\{a \in K^n \mid f_1(a) = 0, \ldots, f_r(a) = 0\} \cup \{a \in K^n \mid g_1(a) = 0, \ldots, g_s(a) = 0\}$
$= \{a \in K^n \mid f_1 g_1(a) = 0, \ldots, f_r g_1(a) = 0, \ldots, f_r g_s(a) = 0\}$

Es gelten:

- $U(1) = R^n$, $U(0) = \emptyset$
- $R^n \setminus U(f) = \{a \in R^n \mid -f(a) \geq 0\}$
- $\{a \in R^n \mid f_1(a) = 0, \ldots, f_r(a) = 0\} = \{a \in R^n \mid (\sum f_i^2)(a) = 0\}$ (d.h. in reellen Körpern werden algebraische Mengen schon von einem einzigen Polynom erzeugt)
- $(R^n \setminus U(f)) \cap (R^n \setminus U(-f)) = \{a \in R^n \mid f(a) = 0\}$ (d.h. algebraische Mengen sind ein Spezialfall von semialgebraischen Mengen)
- $U(f_1) \cap U(f_2) = \{a \in R^n \mid f_1(a) > 0, f_2(a) > 0\}$
- $U(f_1) \cup U(f_2) = \{a \in R^n \mid f_1(a) > 0 \vee f_2(a) > 0\}$
- $U(f)$ ist offen in der (Produkt-)*Intervalltopologie* auf R^n

Definition 2.4. Mengen der Gestalt $U(f_1, \ldots, f_m) = U(f_1) \cap \ldots \cap U(f_m)$ heißen *basisoffen* im R^n.

Bemerkung 2.5. Diese Mengen bilden eine Basis für die Intervalltopologie des R^n.
Die über A semialgebraischen Mengen des R^n bilden eine boolsche Algebra bezüglich $\cap, \cup, R^n \setminus$. Sie sind also insbesondere abgeschlossen unter endlich vielen solcher Operationen.

2.2 Projektionssatz

Satz 2.6 (Projektionssatz). *Sei $S \subseteq R^{n+1}$ eine semialgebraische Teilmenge über A. Dann ist auch*

$$S' = \{(a_1, \ldots, a_n) \in R^n \mid \textit{es gibt } b \in R \textit{ mit } (a_1, \ldots, a_n, b) \in S\}$$

eine semialgebraische Teilmenge über A

Bevor wir uns an den Beweis dieses Satzes machen, wollen wir für allgemeine semialgebraische Mengen eine möglichst übersichtliche Darstellung finden, mit der man dann einfacher arbeiten kann.

Behauptung 2.7. *Jede über A semialgebraische Menge des R^n hat die* ***Normalform***

$$S_1 \cup \ldots \cup S_m$$

mit $S_i = \{a \in R^n \mid g_i(a) = 0, f_{i1}(a) > 0, \ldots, f_{ir_i}(a) > 0\}$
für gewisse $g_i, f_{ij} \in A[X_1, \ldots, X_n]$

Beweis. Sei S boolsche Kombination von Mengen der Gestalt $U(f), f \in A[X_1, \ldots, X_n]$. Wende die de Morgan'sche Regel an (ziehe Komplementbildung korrekt durch die Schnitte und Vereinigungen durch). Distribuiere dann solange aus, bis man S schreiben kann als endliche Vereinigung von Mengen der Gestalt $\{g_1 \not> 0\} \cap \ldots \cap \{g_m \not> 0\} \cap \{f_1 > 0\} \cap \ldots \cap \{f_r > 0\}$. Dann ersetze $\{g \not> 0\}$ durch $(\{-g > 0\} \cup \{g = 0\})$ und distribuiere weiter aus. Dann ist S endliche Vereinigung von Mengen der Gestalt $\{g_1 = 0\} \cap \ldots \cap \{g_m = 0\} \cap \{f_1 > 0\} \cap \ldots \cap \{f_r > 0\}$. Nun ersetze den vorderen Teil (algebraische Menge) durch $\{g = 0\}$ mit $g = \sum g_i^2$. □

Satz 2.8 (Projektionssatz,allgemeine Form). *Seien $g, f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_n, Y]$. Dann gibt es $g_i, f_{ij} \in \mathbb{Z}[X_1, \ldots, X_n]$ mit $1 \leq i \leq s$ und $1 \leq j \leq t_j$, so dass für alle reell abgeschlossenen Körper R und alle $a \in R^n$ gilt:*

$$\exists b \in R\left(g(a,b) = 0 \wedge \bigwedge_{j=1}^{r} f_j(a,b) > 0\right) \Longleftrightarrow \bigvee_{i=1}^{s}\left(g_i(a) = 0 \wedge \bigwedge_{j=1}^{t_i} f_{ij}(a) > 0\right)$$

Wir zeigen nun, wie man den *allgemeinen* Projektionssatz als Verallgemeinerung des Projektionssatzes 2.6 auffassen kann:
Sei $f_{n,d}(C, X)$ das "allgemeine" Polynom vom X-Grad d in den Variablen $X = (X_1, \ldots, X_n)$ mit Koeffizienten $C = (C_1, \ldots, C_N)$ Dabei ist C_i die Unbestimmte, welche als Platzhalter für den Koeffizienten des i-ten X-Monoms fungiert (nachdem man die Monome sinnvoll in einer Reihenfolge geordnet hat). Dabei ist $N = \binom{n+d}{n}$ die Anzahl der Monome vom Grad $\leq d$.

Beispiel 2.9. Für $n = 1$ ist $f_{1,d}(C, X_1) = C_0 + C_1X_1 + \ldots + C_dX_1^d$ und $N = d + 1 = \binom{1+d}{1}$.

Sein nun $S \subseteq R^{m+1}$ eine semialgebraische Menge über A. Diese ist nach Behauptung 2.7 eine Vereinigung von Mengen der Gestalt $\{(a_1, \ldots, a_{m+1}) \in R^{m+1} \mid f_{m+1,d}(c^{(0)}, a) = 0, f_{m+1,d}(c^{(1)}, a), \ldots, f_{m+1,d}(c^{(r)}, a) > 0\}$. Dabei ist d der maximal vorkommende Grad der definierenden Polynome. Die $c^{(i)}$ sind (wie oben) die Koeffizententupel der Länge $N(m + 1, d)$. Nun können wir ohne Beschränkung der Allgemeinheit annehmen, dass S in der Normalformdarstellung 2.7 ist (Man kann sich leicht überlegen, dass die Projektion einer Vereinigung von Mengen gleich der Vereinigung der Projektionen der einzelnen Mengen ist. Für Schnitte gilt dies natürlich nicht, weshalb man nicht noch weiter vereinfachen kann). Die in der Normalform vorkommenden Polynome $g_1, f_{1j} \in A[X_1, \ldots, X_m, Y]$ $(j = 1, \ldots, r)$ kann man mit obiger Überlegung nun als

$$g(c^{(0)}, \ldots, c^{(r)}, X_1, \ldots, X_m, Y),\ f_j(c^{(0)}, \ldots, c^{(r)}, X_1, \ldots, X_m, Y)$$

auffassen, wobei $g, f_j \in \mathbb{Z}[C_0, \ldots, C_{rN(m+1,d)}, X_1, \ldots, X_m, Y]$ für $j = 1, \ldots, r$. (Dabei kommen z.B. in g die letzten $rN(m + 1, d)$ Unbestimmten $C_{N(m+1,d)+1}, \ldots, C_{rN(m+1,d)}$ "nicht wirklich" vor. Analog bei den f_j.) Da die Äquivalenz der Aussagen im allgemeinen Projektionssatz für alle $a \in R^n$ (mit $n = (r+1)N(m+1, d)+m+1$) gilt, so natürlich insbesondere auch für

solche, deren ersten $(r+1)N(m,d)$ Komponenten durch die Koeffizienten (in A) der S-definierenden Polynome festgelegt sind. Dies liefert uns die Aussage von Satz 2.6. Im Unterschied zu 2.6 sagt der allgemeine Porjektionssatz darüber hinaus, dass die S'-definierenden Polynome überhaupt nicht vom reell abgeschlossenen Körper R abhängen (d.h. zwei semialgebraische Mengen S_1, S_2, die über verschiedenen reell abgeschlossenen Körpern R_1 und R_2 (über einem gemeinsamen Unterring A) durch die gleichen Polynome definiert sind, werden auch nach Projektion von den gleichen Polynomen (über A) semialgebraisch definiert).

Beispiel 2.10. Sei $g(X,Y) = X_1 + X_2Y + X_3Y^2 + \ldots + X_{d+1}Y^d$. Für $(a_1,\ldots,a_{d+1}) = a \in K^{d+1}$ (K Unterkörper von R) bedeutet $\exists b\ g(a,b) = 0$, dass $g(a,Y) \in K[Y]$ eine Nullstelle in R hat. Für $d = 2$ kennen wir die äquivalente semialgebraische Formel schon längst: Das Polynom $g(a,Y)$ hat genau dann eine "reelle" Nullstelle, wenn die Diskriminante aus der sogenannten "Mitternachtsformel" größer oder gleich 0 ist (falls der Leitkoeffizient $\neq 0$ ist), oder aber, wenn der Leitkoeffizienten $= 0$ ist und der Linearkoeffizient $\neq 0$, oder wenn alle Koeffizienten $= 0$ sind. Also für $a \in R^3$:

$$\begin{aligned}
&\exists b \in R\ a_3b^2 + a_2b + a_1 = 0\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Leftrightarrow\\
&\big(g_1(a) = 0 \wedge f_{1,1}(a) > 0\big) \vee \big(g_2(a) = 0 \wedge f_{2,1}(a) > 0 \wedge f_{2,2}(a) > 0\big)\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vee\big(g_3(a) = 0 \wedge f_{3,1}(a) > 0\big)\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vee g_4(a) = 0\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{mit } g_1 = X_2^2 - 4X_1X_3,\ f_{1,1} = X_3^2 \text{ (Diskriminante gleich Null)}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad g_2 = 0,\ f_{2,1} = X_2^2 - 4X_1X_3,\ f_{2,2} = X_3^2 \text{ (Diskriminante größer Null)}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad g_3 = X_3,\ f_{3,1} = X_2^2 \text{ ($g(a,Y)$ ist linear, d.h. Nullstelle automatisch)}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad g_4 = X_1^2 + X_2^2 + X_3^2 \text{ ($g(a,Y)$ ist das Nullpolynom)}
\end{aligned}$$

2.3 Beweis des allgemeinen Projektionssatzes

Sei $a \in R^n$ beliebig. Wir wollen nun zeigen, dass es endlich viele Polynomgleichungen und Polynomungleichungen über $\mathbb{Z}[X_1,\ldots,X_n]$ gibt, so dass genau dann immer gewisse Teil(un)gleichungssytem nach Einsetzen von a simultan *wahr* sind, wenn es eine Nullstelle b von $g(a,Y)$ gibt, bei der alle $f_j(a,Y)$ positiv sind.
Wir zeigen zudem, dass diese Polynom(un)gleichungen und die Teilsysteme

unabhängig von a und R sind.
Der Übersicht halber schreiben wir oft $g(Y), f_j(Y)$ statt $g(a,Y), f_j(a,Y)$, vergessen dabei aber nicht, dass, wegen $g, f_j \in \mathbb{Z}[a][Y]$, jede algebraische Verknüpfung (Addition, Multiplikation, Subtraktion) ein Polynom in Y liefert, dessen Koeffizienten selbst Polynome (unabhängig von a) in a über $\mathbb{Z}$ sind. Wir definieren nun

$$n_+(g, f_1, \ldots, f_r) := \#\{b \in R \mid g(b) = 0, f_1(b) > 0, \ldots, f_r(b) > 0\}.$$

Entsprechend betrachten wir für ein beliebiges $h \in \mathbb{Z}[a][Y]$

$$n(g,h) := n_+(g,h) - n_-(g,h)$$
$$\text{mit } n_{+(-)} = \#\{b \in R \mid g(b) = 0, h(b) > (<)0\}$$

Beachte:

- $n(g, f_1^2) + n(g, f_1) = 2n_+(g, f_1)$
- $n(g, f_1^2 f_2^2) + n(g, f_1 f_2^2) + n(g, f_1^2 f_2) + n(g, f_1 f_2) = 2^2 n_+(g, f_1)$
  $\vdots$
- $\sum_{\nu \in \{1,2\}^r} n(g, f_1^{\nu_1} \cdots f_r^{\nu_r}) = 2^r n_+(g, f_1, \ldots, f_r)$

Die Idee ist nun, zu zeigen, dass die einzelnen $n(g,h)$ Polynomfunktionen der Koeffizienten der g, h sind (welche selbst wieder Polynome in den Koeffizienten der g, f_j sind). Die Aussage 'Es gibt eine Nullstelle von g, bei der alle f_j strikt positiv sind' läßt sich schrittweise in Disjunktionen von Aussagen zerlegen von denen dann letztlich gezeigt wird, dass sie Disjunktionen von Konjunktionen von Polynom(un)gleichungen in den a sind (und zwar unabhängig von den a).
Schritt 1: Sei $\deg_Y g(X,Y) = d$. Dann ist die Aussage '*Es gibt eine Nullstelle von $g(a,Y)$, bei der $f_j(a,Y)$ positiv ist*' äquivalent zur Aussage '*Es gibt genau eine oder genau zwei oder ... oder genau d Nullstellen von $g(a,Y)$, bei denen alle $f_j(a,Y)$ positiv sind, oder aber $g(a,Y)$ ist das Nullpolynom und es gibt eine gemeinsame Positivstelle der $f_j(a,Y)$*':

$$\exists b \in R \Big(g(a,b) = 0 \wedge \textstyle\bigwedge_{j=1}^r f_j(a,b) > 0 \Big) \Leftrightarrow$$

$$\Big(\bigvee_{k=1}^{d} 2^r n_+(g, f_1, \ldots, f_r) = 2^r k \Big) \vee \big(g(a,Y) = 0 \wedge \text{alle } f_j(a,Y) \text{ konstant } > 0 \big)$$

$$\vee \quad \big(g(a,Y) = 0 \wedge \ f_j(a,Y) \text{ mit gemeinsamer Positivstelle; nicht alle konstant} \big)$$

(d ist eine obere Schranke für die Anzahl an Nullstellen von g(a,Y)). Die bis jetzt willkürlich erscheinende Fallunterscheidung (alle f_j konstant / ein f_j nicht konstant) erhält im 6. Schritt seine Berechtigung.

Schritt 2: Wir überlegen uns für jede einzelne der $d+2$ Disjunktionen, dass sie in einfachere Teilaussagen weiter zerlegt werden kann. (Die letzten beiden Disjunktionen übergehen wir dabei vorerst.) Dazu überlegen wir uns, dass die Aussage '*Es gibt k verschiedene Nullstellen von $g(a,Y)$, bei der alle $f_j(a,Y)$ positiv sind*' nach unserer Überlegung äquivalent zur Aussage '$\sum_{\nu\in\{1,2\}^r} n(g, f_1^{\nu_1}\cdots f_r^{\nu_r}) = 2^r k$' ist. Da wir auch wissen, dass die Wertemöglichkeiten für jeden einzelnen Summanden durch den Y-Grad von $g(X,Y)$ beschränkt ist (es also nur endlich viele Möglickeiten gibt), kann man die Aussage noch weiter zerlegen, indem man alle *endlich vielen* Möglichkeiten für die Summanden abdeckt, in der Summe die vorgegebene Zahl $2^r k$ anzunehmen. Formal gilt also für jedes $1 \le k \le d$:

$$2^r n_+(g, f_1, \ldots, f_r) = 2^r k \Leftrightarrow \bigvee_{m\in A_k} \bigwedge_{\nu\in\{1,2\}^r} n(g, f_1^{\nu_1}\cdots f_r^{\nu_r}) = m_\nu$$

mit $A_k = \{n \in \mathbb{Z}^{\{1,2\}^r} \mid \sum_{\nu\in\{1,2\}^r} n_\nu = 2^r k \ \wedge\ |n_\nu| \le d\}$

Schritt 3: Zu $a \in R$, d.h. $g, f \in \mathbb{Z}[a][Y]$ berechnen wir jetzt $n(g,f)$ aus den Koeffizienten: Es sei $1 \le \deg(g) = d' \le d$. Betrachte die R-Algebra (zugleich d'-dimensionaler R-Vektorraum):

$$R[Y]/(g) = R \oplus Ry \oplus Ry^2 \oplus \ldots \oplus Ry^{d'-1} = V$$

mit $y := Y + (g)$. Wir definieren uns nun zu f und den d' Nullstellen $\alpha_1, \ldots, \alpha_{d'} \in \overline{R}^{alg} = R(\sqrt{-1})$ von g (mit Vielfachheit) eine symmetrische Bilinearform

$$\begin{aligned} b_f : V \times V &\longrightarrow R \\ (h_1 + (g), h_2 + (g)) &\mapsto \sum_{i=1}^{d'} f(\alpha_i) h_1(\alpha_i) h_2(\alpha_i) \end{aligned}$$

Die Wohldefiniertheit, Symmetrie und R-Bilinearität ist sofort ersichtlich; dass die Bilder alle aus R sind, sieht man durch komplexes Konjugieren des Ausdrucks und Berücksichtigung der Tatsache, dass mit α auch $\bar{\alpha}$ Nullstelle von g (mit gleicher Vielfachheit) ist. Sei M die Matrixdarstellung von b_f bezgl. der kanonischen Basis $(1, y, \ldots, y^{d'-1})$ von V. Die folgenden Fakten gelten über jedem reell abgeschlossenen Körper R:

(1) b_f-*Orthogonalisierung*: es gibt eine Basis $(v_1, \ldots, v_{d'})$ von V mit $b_f(v_i, v_j) = 0$ für $i \neq j$ (bzw. es gibt eine "reelle" invertierbare Matrix C, sodass CMC^T Diagonalgestalt hat).

(2) Signatur$(b_f) := \#\{i \mid b_f(v_i, v_i) > 0\} - \#\{i \mid b_f(v_i, v_i) < 0\}$ ist unabhängig von der Wahl der b_f-orthogonalen Basis $(v_1, \ldots, v'_d)$ *(Trägheitssatz von Sylvester)*, und ist damit wohldefiniert.

(3) Es gibt sogar schon eine "orthogonale" Matrix C (d.h. $C^{-1} = C^T$), sodass $CMC^T = CMC^{-1}$ Diagonalgestalt hat *(Hauptachsentransformation)*. In der Diagonalen stehen die Nullstellen des charakteristischen Polynoms χ_M von M.
Also Signatur(b_f) = #{positive EW von M (mit Vielfachheit)} − #{negative EW von M (mit Vielfachheit)}.

(4) *Descartes'sche Regel*: #{ positive Nullstellen von χ} − #{ neg. Nullstellen von χ}(alle mit Vielfachheit)= #{Vorzeichenwechsel der Koeffizientenfolge von $\chi(t)$} − #{Vorzeichenwechsel der Koeffizientenfolge von $\chi(-t)$} für Polynome $\chi \in R[t]$, welche über R in Linearfaktoren zerfallen.

(5) *Satz von Rolle*: Seien $f, g \in R[X]$ und $a < b \in R$ mit $f(a) = f(b) = 0$, $g(x) \neq 0$ auf $[a, b]$ und $f(x) \neq 0$ auf $]a, b[$. Dann gibt es ein $x \in [a, b]$ mit $(\frac{f}{g})'(x) = 0$

Satz 2.11. $n(g, f) = \text{Signatur}(b_f)$

Beweis. Wir suchen eine passende b_f-Orthogonalbasis von V: Die *verschiedenen* Nullstellen von g seien $\alpha_\nu = a_\nu + ib_\nu$. Für $\nu = 1, \ldots, m \leq d'$ seien diejenigen Nullstellen indiziert, für die $b_\nu \geq 0$ ist. Zu jedem Nullstellen"paar" $\alpha_\nu, \overline{\alpha_\nu}$ mit $\nu \leq m$ basteln wir uns nun ein Polynom:

1.Fall: $\alpha_\nu = \overline{\alpha_\nu}$, d.h. $\alpha_\nu \in R$
Wähle $v + (g) \in V$ mit $v(\alpha_\nu) = 1$ und $v(\alpha) = 0$ für jede g-Nullstelle $\alpha \neq \alpha_\nu$, z.B.

$$v(Y) := \prod_{\alpha \neq \alpha_\nu} \frac{Y - \alpha}{\alpha_\nu - \alpha}$$

Dieses Polynom ist reell, da Anwenden der Konjugation nur Faktoren permutiert und somit das Polynom insgesamt invariant läßt. Es gilt

$b_f(v,v) = \sum_\alpha \mu_\alpha f(\alpha) v(\alpha)^2 = \mu_{\alpha_\nu} f(\alpha_\nu)$, wobei μ_α die Vielfachheit der Nullstelle α bezeichne. Also gilt:

$$\text{Signatur}(b_f(v,v)) = \begin{cases} 1 & : \quad f(\alpha_\nu) > 0 \\ 0 & : \quad f(\alpha_\nu) = 0 \\ -1 & : \quad f(\alpha_\nu) < 0 \end{cases} \tag{1}$$

Setze $W_\nu := \text{Span}_R\{v\}$.

2.Fall: $\alpha_\nu \notin R$, d.h. $b_\nu > 0$
Wähle $u_1 + (g), u_2 + (g) \in V$ mit

$$\begin{aligned} u_1(\alpha_\nu) &= 1 &&= u_1(\overline{\alpha_\nu}) \\ u_2(\alpha_\nu) &= i &&= \overline{u_2(\overline{\alpha_\nu})} \\ u_{1,2}(\alpha) &= 0 \quad \text{für } \alpha \neq \alpha_\nu \end{aligned}$$

z.B. für

$$\begin{aligned} u_1 &:= \frac{1}{4b_\nu^2}\left(\big(Y - \overline{\alpha_\nu}\big)^2 \prod_{\alpha \neq \alpha_\nu, \overline{\alpha_\nu}} \frac{Y-\alpha}{\alpha_\nu - \alpha} + \big(Y - \alpha_\nu\big)^2 \prod_{\alpha \neq \alpha_\nu, \overline{\alpha_\nu}} \frac{Y-\alpha}{\overline{\alpha_\nu} - \alpha} \right) \\ u_2 &:= \frac{1}{2b_\nu}\left(\big(Y - \overline{\alpha_\nu}\big) \prod_{\alpha \neq \alpha_\nu, \overline{\alpha_\nu}} \frac{Y-\alpha}{\alpha_\nu - \alpha} + \big(Y - \alpha_\nu\big) \prod_{\alpha \neq \alpha_\nu, \overline{\alpha_\nu}} \frac{Y-\alpha}{\overline{\alpha_\nu} - \alpha} \right) \end{aligned}$$

Beide Polynome sind invariant unter (komplexer) Konjugation (der eine Summand ist gerade das komplex Konjugierte des anderen Summanden). Die Auswertungsbedingung an den Nullstellen α von g rechnet man ebenfalls schnell nach (Erinnerung: $z - \overline{z} = 2i\text{Im}(z)$).
Es gilt

$$\begin{aligned} b_f(u_1,u_1) &= \sum_\alpha \mu_\alpha f(\alpha) u_1(\alpha)^2 = \mu_{\alpha_\nu}\big(f(\alpha_\nu) + f(\overline{\alpha_\nu})\big) \\ b_f(u_2,u_2) &= \sum_\alpha \mu_\alpha f(\alpha) u_2(\alpha)^2 = \mu_{\alpha_\nu}\big(-f(\alpha_\nu) - f(\overline{\alpha_\nu})\big) \end{aligned}$$

u_1, u_2 sind R-linear unabhängig, da jede "echte" "reelle" Linearkombination von ihnen einen Wert $\neq 0$ an der Stelle α_ν annimmt. $b_f \restriction \text{Span}\{u_1,u_2\}$ hat Signatur 0, da die zugehörige 2×2 -Matrix die Gestalt $M = \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix}$ hat, und somit für das charakteristische Polynom $\chi \in R[t]$ gilt: $\chi(t) = \chi(-t)$, d.h. es gibt für jede positive Nullstelle eine negative Nullstelle und umgekehrt. Setze $W_\nu := \text{Span}_R\{u_1,u_2\}$.

Setze jetzt noch $U := \{w + (g) \in V \mid w(\alpha) = 0 \textit{ für alle } \text{Nullstellen } \alpha \text{ von } g\}$. Dann gilt $W_1 \perp \ldots \perp W_m \perp U = V$. Dabei ist $\perp$ die b_f-orthogonale (und auch direkte!) Summe.
"$\subset$": trivial
"$\supset$": sei $h_1 + (g) \in V$. Bastele $h_2 + (g) \in W_1 \perp \ldots \perp W_m$ mit $h_1(\alpha) = h_2(\alpha)$ für alle Nullstellen α von g. $\Rightarrow h_1 = h_2 + (h_1 - h_2) \Rightarrow h_1 + (g) = \underbrace{h_2 + (g)}_{\in \bigoplus W_i} + \underbrace{(h_1 - h_2) + (g)}_{\in U}$. (Sich zu überlegen, dass es möglich ist sich ein solches Polynom aus den $\bigoplus W_i$ zu 'basteln' ist eine einfache Übung).
Die Gesamtsignatur ergibt sich dann als Summe der Signaturen von b_f eingeschränkt auf die Teilräume (leicht zu sehen; man setze sich einfach eine Basis aus "Orthogonal"-Basen der Teilräume zusammen). $b|_U \equiv 0$, also ist auch die Signatur ist null. Wie gezeigt, verschwindet auch die Signatur von $b|_{W_\nu}$, falls $\alpha_\nu \notin R$. Somit spielen also nur die Räume zu den "reellen" Nullstellen α von g eine Rolle. Mit Gleichung 1 folgt die Behauptung. □

Wie wir im 5. Schritt noch sehen werden, läßt sich die Aussage 'Signatur der symmetrischen Matrix M nimmt den gegebenen Wert μ an' äquivalent umformulieren in polynomiale (Un-)Gleichungssysteme über $\mathbb{Z}$ für die Koeffizienten des charakteristischen Polynoms, welche sich ihrerseits polynomial aus den Einträgen der Matrix berechnen. Wir müssen also zunächst zeigen, dass die Einträge der Matrix M zu b_f sich als Polynome (über $\mathbb{Z}$) in den *Koeffizienten* von g, f berechnen lassen.
Schritt 4: Berechnung von $M = \left(b_f(y^i, y^j)\right)_{0 \le i,j \le d'-1}$, wobei $1, y, \ldots, y^{d'-1}$ die kanonische Basis von V ist.

$$b_f(y^i, y^j) = \sum_{\substack{\text{Nst. } \alpha \text{ von } g \\ \text{mit Vielfachh.}}} f(\alpha)\alpha^{i+j} = \sum_{\mu=0}^{l} e_\mu \sum_{\substack{\alpha \\ \text{mit Vfh.}}} \alpha^{i+j+\mu}, \tag{2}$$

falls $f = e_l Y^l + e_{l-1} Y^{l-1} + \ldots + e_0$. Das Problem ist nun, dass wir die Matrixeinträge ja aus den *Koeffizienten* der Polynome g, f berechenen wollen, wir aber bisher nur eine Berechnung aus den Koeffizienten von f und den *Nullstellen* von g haben. Spätestens aus der Algebra-Vorlesung wissen wir aber, dass sich Nullstellen eines Polynoms nicht allgemein als Polynome in den Koeffizienten berechnen lassen (noch nicht einmal mit Radikalen). Hier haben wir aber Glück, denn die $\sum_{\alpha \text{ mit Vfh.}} \alpha^{i+j+\mu}$ aus den $b_f(y^i, y^j)$ sind nicht irgendwelche Polynome in den Nullstellen, sondern sogar *symmetrisch* in den

α_i (mit Vfh.) über $\mathbb{Z}$, d.h. man kann im Polynom zwei beliebige α_i, α_j vertauschen, und das Polynom ist immer noch dasselbe (wenn man mal kurzfristig so tut, als seien die α_i Unbestimmte). Es gibt einen bekannten Satz über symmetrische Polynome, der in unserem Fall folgendes besagt:

Bemerkung 2.12. Jedes symmetrische Polynom $h(t_1, \ldots, t_m) \in \mathbb{Z}[t_1, \ldots, t_m]$ kann geschrieben werden als $h^*(s_1, \ldots, s_m)$ mit $h^* \in \mathbb{Z}[S_1, \ldots, S_m]$ und $s_i = \sum_{1 \le l_1 < \ldots < l_i \le m} t_{l_1} \cdots t_{l_i} \in \mathbb{Z}[t_1, \ldots, t_m]$. Die s_i werden *elementarsymmetrische* Polynome genannt. Einen Beweis dafür findet man etwa in [Kunz,Algebra].

Beachte:

$$\begin{aligned} g = g(a, Y) &= c_{d'} \prod_{\alpha_i \text{ mit Vfh.}} (Y - \alpha_i) \\ &= c_{d'} \big(Y^{d'} - (\alpha_1 + \ldots + \alpha_{d'}) Y^{d'-1} + \ldots + (-1)^{d'} (\alpha_1 \cdots \alpha_{d'}) \big) \\ &= c_d \big(Y^{d'} - s_1(\alpha_1, \ldots, \alpha_{d'}) Y^{d'-1} + \ldots + (-1)^{d'} s_{d'}(\alpha_1, \ldots, \alpha_{d'}) \big) \end{aligned}$$

Andererseits ist $g(a, Y) = c_{d'} Y^{d'} + \ldots + c_0$, also folgt $s_i(\alpha_1, \ldots, \alpha_{d'}) = (-1)^i \frac{c_{d'-i}}{c_{d'}}$, und somit erhält man, wenn man in obigem Ausdruck 2 die symmetrischen Summen $\sum_{\alpha \text{ mit Vfh}} \alpha^{i+j+\mu}$ durch die jeweilige Darstellung $h^*(s_1, \ldots, s_m)$ ersetzt:

Folgerungen 2.13. Die Einträge $b_f(y^i, y^j)$ der Matrix M sind Polynome über $\mathbb{Z}$ in den Koeffizienten von g und f und $\frac{1}{c_{d'}}$ (dem inversen Leitkoeffizienten von g). Ganz am Schluss muß man also die vorkommenden (Un-)Gleichungen noch vom "Nenner" $c_{d'}$ befreien, indem man sie mit einer hinreichend großen (geraden) Potenz von $c_{d'}$ durchmultipliziert. ('Gerade Potenz', damit man uniform mit etwas Positivem multipliziert und die Ungleichungen nicht "zerstört").

Schritt 5: Sei χ das charakteristische Polynom von M, so folgt mit Fakt (3),(4) und Satz 2.11: $n(g, f) = \mu \Leftrightarrow \#\{\text{VZW der Koeffizienten von } \chi(t)\} - \#\{\text{VZW der Koeffizienten von } \chi(-t)\} = \mu$. Sowohl die Koeffizienten von $\chi(t)$, als auch die von $\chi(-t)$ lassen sich polynomial über $\mathbb{Z}$ aus den Einträgen von M berechenen (die ihrerseits selbst wieder polynomial aus den ... usw.) Die Frage, auf die nun alles hinausläuft ist, ob die (endlich vielen!) Alternativen für die Anzahl der entsprechenden Vorzeichenwechsel jeweils äquivalent sind zu einer boolschen Kombination von Polynomungleichungen über $\mathbb{Z}$ in den Koeffizienten von $\chi(t), \chi(-t)$:

Sei etwa $\chi(t) := \beta_{d'}t^{d'} + \beta_{d'-1}t^{d'-1} + \ldots + \beta_0$. Dann ist z.B.
$\#\{\text{VZW der Koeffizienten von } \chi(t)\} = 1$ äquivalent zur Aussage

$$
\begin{aligned}
& \Big(\beta_{d'}\beta_{d'-1} < 0 \wedge \bigwedge_{j<d'-1} \beta_{d'-1}\beta_j \geq 0\Big) \\
\vee\ & \Big(\beta_{d'-1} = 0 \wedge \beta_{d'}\beta_{d'-2} < 0 \wedge \bigwedge_{j<d'-2} \beta_{d'-2}\beta_j \geq 0\Big) \\
\vee\ & \\
\vdots\ & \\
\vee\ & \Big(\beta_{d'}\beta_{d'-1} \geq 0 \wedge \beta_{d'-1}\beta_{d'-2} < 0 \wedge \bigwedge_{j<d'-2} \beta_{d'-2}\beta_j \geq 0\Big) \\
\vee\ & \Big(\beta_{d'}\beta_{d'-1} \geq 0 \wedge \beta_{d'-2} = 0 \wedge \beta_{d'-1}\beta_{d'-3} < 0 \wedge \bigwedge_{j<d'-3} \beta_{d'}\beta_j \geq 0\Big) \\
\vee\ & \\
\vdots\ & \\
\vee\ & \Big(\bigwedge_{j>1} \beta_j\beta_1 \geq 0 \wedge \beta_1\beta_0 < 0\Big)
\end{aligned}
$$

Es ist dem Leser überlassen sich davon zu überzeugen, dass jede andere Anzahl an Vorzeichenwechsel ebenfalls durch ein (noch komplizierteres) Polynom(un)gleichungssystem in den β_i wie oben beschrieben werden kann.
Nun haben wir also tatsächlich die gesamte ursprüngliche Aussage

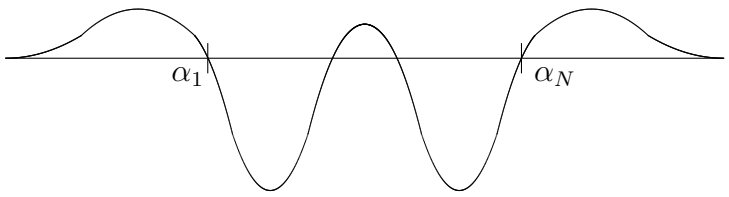
$$\exists b \in R\ \big(g(a,b), f_j(a,b) > 0\big)$$

stufenweise auf ein semialgebraisches Polynomungleichungssystem über $\mathbb{Z}$ zurückgeführt. Leider hängt dieses bis jetzt noch von $a \in R^n$ ab. Wir haben zwar mit einem ganz allgemeinen a gearbeitet, aber an einer Stelle haben wir doch eine spezielle Eigenschaft von a benötigt, als wir nämlich $d' := \deg_Y g(a,y)$ gesetzt haben. d' war dann die Dimension des Vektorraumes V und somit die Größe der Matrix M, von der natürlich dann auch Anzahl und "Struktur" der Koeffizienten ihres charakteristischen Polynoms abhängt. Wir haben uns also bisher für ein allgemeines $1 \leq d' \leq d$ überlegt, dass für alle a mit $\deg_Y g(a,Y) = d'$ die Nullstellenaussage aus dem Satz äquivalent zu einem festen semialgebraischen (Un-)Gleichungssystem über $\mathbb{Z}$ ist.

Schritt 6: Zusammenfassung und Sonderfall $g(a,Y)=0$:
Bisher haben wir also zu $g, f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_n, Y]$ gewisse $g_{d',i}, f_{d',ij} \in \mathbb{Z}[x_1, \ldots, X_n]$ für $1 \leq d' \leq d$, so dass für alle R und alle $a \in R$ gilt:

$$\begin{aligned} & \exists b \in R\Big(g(a,b)=0 \wedge \bigwedge_j f_j(a,b)>0\Big) \\ \iff \quad & \bigvee_{d'=1}^{d} \bigvee_{i=1}^{s_{d'}} \Big(g_{d',i}(a)=0 \wedge \bigwedge_j f_{d',ij}(a)>0 \wedge \ \deg_Y g(a,Y)=d'\Big) \\ & \vee \text{ (noch zu überlegendes Kriterium im Fall } g(a,Y)=0) \end{aligned}$$

Glücklicherweise ist es nicht allzu schwierig die Aussage '$\deg_Y g(a,Y)=d'$' semialgebraisch über $\mathbb{Z}$ umzuformulieren. Ist z.B. $g(X,Y)=c_d(X)Y^d+\ldots+c_0(X)$, so ist die Aussage gleichbedeutend mit $c_d(a)=0 \wedge \ldots \wedge c_{d'+1}(a)=0 \wedge c_{d'}(a)\neq 0$, was nach unseren allgemeinen Überlegungen zu Beginn des Kapitels auf "Normalform" umgeformt werden kann. Bleibt also nur noch zu überlegen, was man im Fall $g(a,Y)=0$, d.h. $c_d(a)=0,\ldots,c_0(a)=0$ macht. Die bisherigen Überlegungen greifen hier nicht, da $V=R[Y]/(0)\cong R[Y]$ ja nicht endlichdimensional ist. Die Idee ist, sich aus den f_i ein "Ersatz"-g mit Y-Grad ≥ 1 zu konstruieren, bei dem aufgrund der Konstruktion schon garantiert ist, dass *wenn* die $f_j(a,Y)$ eine gemeinsame Positivstelle in R haben, das Ersatz-$g(a,Y)$ eine Nullstelle hat, bei der die $f_j(a,Y)$ positiv sind. Wir setzen noch voraus, dass nicht alle $f_j(a,Y)$ konstant sind. (Den trivialen Unterfall, daß alle $f_j(a,Y)$ konstant sind, muß man nochmals gesondert betrachten.) Setze $f:=f_1(a,Y)\cdots f_r(a,Y)$. Seien zu $a\in R^n$ die Nullstellen von $f(a,Y)=f$ in R mit $\alpha_1<\ldots<\alpha_N$ bezeichnet, wobei $N\in\mathbb{N}$ ist. Diese unterteilen R in Teilintervalle, auf denen die Funktion f konstantes Vorzeichen hat. Nun gehen wir zur rationalen Funktion $\frac{f}{1+f^2}$ über. Diese hat die gleichen Nullstellen wie f und ist an den gleichen Stellen positiv/negativ. Wenn wir so tun als hätten wir es mit dem Fall $R=\mathbb{R}$ zu tun, wird die Idee anschaulich klar: Anders als die Funktion f geht $\frac{f}{1+f^2}(y)$ für $|y|\to\infty$ asymptotisch gegen 0. Wenn alle $f_j(a,Y)$ eine gemeinsame Positivstelle haben, so nimmt die Funktion $\frac{f}{1+f^2}$ also garantiert ein lokales Maximum in den Intervallen an, in denen alle $f_j(a,Y)$ positive Werte annehmen. (Denn, wenn ein f_j sein Vorzeichen an einer Stelle wechselt, hat $\frac{f}{1+f^2}$ an dieser Stelle schon eine Nullstelle). Also gibt es in einem solchen Intervall eine Nullstelle von $(\frac{f}{1+f^2})'$.



Für den Fall, dass es sich um ein Intervall der Form $[\alpha_j, \alpha_{j+1}]$ handelt, folgt dies schon aus dem Satz von Rolle, welcher auch für beliebige reell abgeschlossene $R \neq \mathbb{R}$ gilt (siehe Fakt (5)). Sollten die Intervalle, auf denen $f_1(a,Y), \ldots, f_r(a,Y)$ positiv sind, von der Form $(-\infty, a_1]$,$[a_N, \infty)$ oder $(-\infty, \infty)$ sein, so hilft hier auch der Satz von Rolle weiter, indem man für einen positiven Wert p, den $\frac{f}{1+f^2}$ in einem solchen Intervall annimmt, einfach die Funktion $\frac{f}{1+f^2} - \frac{p}{2}$ anschaut. Diese hat links und rechts von einer Stelle x mit $\frac{f}{1+f^2}(x) = p$ eine Nullstelle. Dazu überlege man sich selbst, dass $|\frac{f}{1+f^2}| \leq \frac{2}{|f|}$ und andererseits $|f(x)| > p$ für hinreichend großes x. Setzt man nun $g^* := (1-f^2)f' = (\frac{f}{1+f^2})'(1+f^2)^2$ (Quotientenregel anwenden), so greift das bisher überlegte Verfahren für g^* statt g. Natürlich hängt der Grad von $g^*(Y)$ jetzt von den möglichen Graden von $f_j(a,Y)$ ab, d.h. wie zuvor für $g(a,Y)$ müssen nun noch alle Gradmöglichkeiten der $f_j(a,Y)$ separat bedacht werden, was aber ja semialgebraisch möglich ist. Dabei muss der Fall "$f_j(a,Y) = 0$ für ein j" ausgeschlossen und der (triviale) Fall "$f_j(a,Y) = const.$ für alle j" gesondert behandelt werden. Dies sei hier aber nicht weiter ausgeführt, da es die gleichen Überlegungen wie zu Beginn von Schritt 6 erfordert.

Zum Abschluß des Beweises, wollen wir nun noch den Beweis zu den Punkten (4) und (5) aus der Faktensammlung nachtragen.

zu (4):

Lemma 2.14. *Sei $\varphi(t) \in R[t] \setminus \{0\}$ und dessen Koeffizientenfolge habe ν Zeichenwechsel. Dann besitzt $\varphi(t)(t-c)$ mit $c > 0$ in seiner Koeffizientenfolge mindestens $\nu + 1$ Zeichenwechsel.*

Beweis. Induktion über den Grad d von $\varphi(t)$:
$\underline{d=0}$: $\varphi(t) = a_0$. Aussage ist offensichtlich wahr.
$\underline{d \to d+1}$: Sei $\varphi(t) = a_{d+1}t^{d+1} + \ldots + a_1 t + a_0$ mit ν VZW. Sei o.B.d.A $a_0 \neq 0$, sonst kann man ein t ausfaktorisieren und ist somit im Fall der Induktionsvoraussetzung d.

$$\varphi(t)(t-c) = t(t-c)(a_{d+1}t^d + \ldots + a_1) + (t-c)a_0.$$

Falls $a_0 a_1 > 0$, so ist $\#\text{VZW}(a_{d+1}t^d + \ldots + a_1) = \nu$,
falls $a_0 a_1 < 0$, so ist $\#\text{VZW}(a_{d+1}t^d + \ldots + a_1) = \nu - 1$ und,
falls $a_1 = 0$, so hat $(a_{d+1}t^d + \ldots + a_1)$ mindestens $\nu - 1$ VZW.
Auf den vorderen Summanden $t(t-c)(a_{d+1}t^d + \ldots + a_1)$ können wir die Induktionsvoraussetzung anwenden(multiplizieren mit t ändert nichts an der Anzahl der VZW der Koeffizienten). Schreiben wir also für den ersten Summanden $b_{d+2}t^{d+2} + \ldots + b_1 t$. Mit der Induktionsvoraussetzung folgt für $b_{d+2}t^{d+2} + \ldots + b_1 t$ jeweils:

$$\#\text{VZW} \geq \begin{cases} \nu + 1 & : \quad a_0 a_1 > 0 \\ \nu - 1 + 1 & : \quad a_0 a_1 < 0 \\ \nu - 1 + 1 & : \quad a_1 = 0 \end{cases}$$

Betrachte $\varphi(t)(t-c) = b_{d+2}t^{d+2} + \ldots + b_2 t^2 + (b_1 + a_0)t - ca_0$.

Im Fall $(a_0 a_1 < 0)$ haben, wegen $b_1 = -ca_1$, die Elemente b_1 und a_0 das gleiche Vorzeichen und somit auch $b_1 + a_0$ das gleiche wie b_1. Jedoch ist das Vorzeichen von $-ca_0$ entgegengesetzt, d.h. die gesamte Koeffizientenfolge hat mindestens $\nu + 1$ VZW.

Im Fall $(a_0 a_1 > 0)$ hat entweder $b_1 + a_0$ das gleiche Vorzeichen wie b_1, oder aber $-ca_0$ hat entgegengesetztes Vorzeichen zu $b_1 + a_0$. Beide Male gibt es jedenfalls mindestens $\nu + 1$ VZW.

Im Fall $a_1 = b_1 = 0$ ist

$$\#\text{VZW}(b_{d+2}, \ldots, b_2, a_0, -ca_0) \geq \nu + \#\text{VZW}(a_0, -ca_0) = \nu + 1.$$

□

Beweis. (der Descartes'schen Regel, Fakt (4))
Alle Nullstellen von $\varphi(t)$ seien aus R. Sei o.B.d.A. $\varphi(t)$ normiert:

$$\varphi(t) = \underbrace{\prod_{i=1}^{n}(t+\alpha_i)}_{\psi_1(t)} \underbrace{\prod_{j=1}^{m}(t-\beta_j)}_{\psi_2(t)} \text{ für } \alpha_i, \beta_j > 0$$

$\psi_1(t)$ hat 0 Vorzeichenwechsel $\overset{\text{Lemma 2.14}}{\Longrightarrow}$ $\varphi(t)$ hat $\geq m$ Vorzeichenwechsel.
$\psi_2(-t)$ hat 0 Vorzeichenwechsel $\overset{\text{Lemma 2.14}}{\Longrightarrow}$ $\varphi(-t)$ hat $\geq n$ Vorzeichenwechsel.
Es gilt $\deg(\varphi) = n + m \leq \#\text{ VZW}(\varphi(t)) + \#\text{ VZW}(\varphi(-t)) \leq \deg\varphi$, also
$\#\text{ VZW}(\varphi(t)) = \#\{\text{positive Nullstellen von } \varphi\}$ und
$\#\text{ VZW}(\varphi(-t)) = \#\{\text{negative Nullstellen von } \varphi\}$. □

zu (5): Sei $r(X) = \dfrac{f(X)}{g(X)} \in R(X)$ mit $g(x) \neq 0$ auf $[a,b]$, $f(x) \neq 0$ auf $]a,b[$ und $f(a) = f(b) = 0$.
Wegen $r(a) = 0$, folgt $r = (X-a)^m s(X)$ für ein $s \in R(X)$ mit $s(a) \neq 0$.

$$\Rightarrow\ r' = m(X-a)^{m-1}s(X) + (X-a)^m s'(X)$$
$$\Rightarrow\ \frac{r'}{r} = \frac{m}{(X-a)} + \frac{s'}{s}.$$

Die gleiche Überlegung für $r(b) = 0$ liefert $\dfrac{r'}{r} = \dfrac{n}{(X-b)} + \dfrac{t'}{t}$.

Sei $\dfrac{s'}{s} = \dfrac{h_1}{h_2}$ für gewissen *Polynome* $h_1, h_2 \in R[X]$ mit $h_2(a) \neq 0$.
Für $0 < \epsilon < 1$ lässt sich mit Hilfe der Dreiecksungleichung (die natürlich für Beträge in jedem angeordneten Körper gilt) $|h_1(a+\epsilon)|$ wie folgt nach oben abschätzen:
$|h_1(a+\epsilon)| \leq \max\{\text{Beträge der Koeffizienten von } h_1\}(|a|+1)^{\deg(h_1)}$.
Sei e der minimale Abstand von a zu den reellen Nullstellen von h_2, dann lässt sich für $0 < \epsilon < \frac{e}{2}$ eine Abschätzung nach unten finden: Es gilt ja $h_2(X) = \gamma\prod_{i=1}^{l}(X-\alpha_i)\prod_{i=1}^{q}\left((X-\beta_i)^2+\delta_i^2\right)$ mit $\delta_i \neq 0$.
Also $|h_2(a+\epsilon)| \geq (\frac{e}{2})^l \prod_{i=1}^{q}\delta_i^2$. Insgesamt hat man also, dass $\dfrac{s'}{s}$ in einer Intervallumgebung von a beschränkt bleibt. Analoges gilt für $\dfrac{t'}{t}$ an der Stelle b, so dass wir nun folgendes formulieren können:
Man findet $c < d \in]a,b[$ mit

- c so nahe an a, dass $\frac{r'}{r}(c) > 0$, und
- d so nahe an b, dass $\frac{r'}{r}(d) < 0$.

$r(c)$ und $r(d)$ haben aber gleiches Vorzeichen, also gilt $r'(c)r'(d) < 0$. Nun gilt der *Zwischenwertsatz* in reell abgeschlossenen Körpern nicht nur für Polynome, sondern auch für rationale Funktionen, deren Nenner im entsprechenden abgeschlossenen Intervall keine Nullstelle hat (Man kann ja mit dem Quadrat des Nenners multiplizieren, Zwischenwertsatz für Polynome anwenden und dann wieder durch das Quadrat des Nenners teilen). $r' = \frac{f'g - fg'}{g^2}$ ist eine solche rationale Funktion. Also hat r' eine Nullstelle in $]c, d[\subset [a, b]$.

2.4 Anwendungen des Projektionssatzes

Satz 2.15 (Übertragungssatz (für Nullstellen von Polynomen)). *Seien (R_l, R_l^2) für $l = 1, 2$ reell abgeschlossene Oberkörper eines angeordneten Körpers (K, P) mit $R_1^2 \cap K = P = R_2^2 \cap K$. Sei $p \in K[X]$. Dann gilt: Hat p eine Nullstelle in R_1, so auch in R_2.*

Beweis. $p = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, $a_i \in K$, $a := (a_0, \ldots, a_{n-1})$. Mit dem allgemeinen Projektionssatz folgt

$$\{a \in R_l^n \mid \exists b \in R_l \; p(a, b) = 0\} = \bigcup_i \{a \in R_l^n \mid g_i(a) = 0 \bigwedge_j f_{ij}(a) > 0\}$$

für $p = X^n + X_{n-1}X^{n-1} + \ldots + X_0$ und gewisse $g_i, f_{ij} \in \mathbb{Z}[X_0, \ldots, X_{n-1}]$, welche unabhängig von R sind. Also gilt für $a \in K$:

$$\exists b \in R_1 \; p(a, b) = 0 \Leftrightarrow \bigvee_i \big(g_i(a) = 0 \wedge \bigwedge_j f_{ij} > 0\big) \Leftrightarrow \exists b \in R_2 \; p(a, b) = 0$$

□

Durch *Iteration* des allgemeinen Projektionssatzes erhält man:

Bemerkung 2.16. Zu $g, f_j \in \mathbb{Z}[X_1, \ldots, X_n, Y_1, \ldots Y_m]$ gibt es $g_i, f_{ij} \in \mathbb{Z}[X_1, \ldots, X_n]$, so dass für alle reell abgeschlossenen Körper R und alle $a \in R^n$ gilt:

$$\exists b_1, \ldots, b_m \in R \; \big(g(a, b) = 0 \wedge \bigwedge_j f_j(a, b) > 0\big) \Leftrightarrow \bigvee_i \big(g_i(a) = 0 \wedge \bigwedge_j f_{ij}(a) > 0\big)$$

Beweis. Induktion über m:

$$\begin{aligned}
& \exists b_1, \dots, b_m \big(g(a,b) = 0 \wedge \bigwedge_j f_j(a,b) > 0 \big) \\
\Leftrightarrow \quad & \exists b_m \Big(\exists b_1, \dots, b_{m-1} \big(g(a, b_1, \dots, b_{m-1}, b_m) = 0 \wedge \dots \big) \Big) \\
\Leftrightarrow \quad & \exists b_m \Big(\bigvee_i \big(\tilde{g}_i(a, b_m) = 0 \wedge \bigwedge_j \tilde{f}_{ij}(a, b_m) > 0 \big) \Big) \\
\Leftrightarrow \quad & \bigvee_i \exists b_m \big(\tilde{g}_i(a, b_m) = 0 \wedge \bigwedge_j \tilde{f}_{ij}(a, b_m) > 0 \big) \\
\Leftrightarrow \quad & \bigvee_i \bigvee_\nu \big(\tilde{g}_{i\nu}(a) = 0 \wedge \bigwedge_j \tilde{f}_{i\nu j}(a) > 0 \big)
\end{aligned}$$

□

Korollar 2.17. *Sei (K, P) gemeinsamer angeordneter Unterkörper der reell abgeschlossenen Körper R_1, R_2. Für jede über K semialgebraische Menge S gilt dann:*

$$S(R_1) \neq \emptyset \Leftrightarrow S(R_2) \neq \emptyset$$

Beweis. Sei S definiert durch $\bigvee_i \big(g_i(a, Y) = 0 \wedge \bigwedge_j f_{ij}(a, Y) > 0 \big)$, d.h. $S(R) := \{ b \in R^m \mid \bigvee_i \big(g_i(a,b) = 0 \wedge \bigwedge_j f_{ij}(a,b) > 0 \big) \}$ für gewisse $g_i, f_{ij} \in \mathbb{Z}[X_1, \dots, X_n, Y_1, \dots, Y_m]$ und ein $a \in K^n$.

$$\begin{aligned}
S(R_1) \neq \emptyset \quad & \Longleftrightarrow \quad \exists b \in R_1^m \bigvee_i \Big(g_i(a,b) = 0 \wedge \bigwedge_j f_{ij}(a,b) > 0 \Big) \\
& \overset{\text{Bem. 2.16}}{\Longleftrightarrow} \quad \bigvee_i \big(\tilde{g}_i(a) = 0 \wedge \bigwedge_j \tilde{f}_{ij}(a) > 0 \big) \\
& \overset{\text{Bem. 2.16}}{\Longleftrightarrow} \quad \exists b \in R_2^m \bigvee_i \Big(g_i(a,b) = 0 \wedge \bigwedge_j f_{ij}(a,b) > 0 \Big) \\
& \Longleftrightarrow \quad S(R_2) \neq \emptyset
\end{aligned}$$

□

2.4.1 Anwendungsbeispiel: Das 17. Hilbertsche Problem (1900)

Gegeben: $f \in \mathbb{R}[X_1, \dots, X_n]$ positiv semidefinit, d.h. $f(a) \geq 0$ für alle $a \in \mathbb{R}^n$.

Frage: Gibt es $N \in \mathbb{N}$, $g_i, h_i \in \mathbb{R}[X_1, \ldots, X_n]$ mit

$$f = \sum_{i=1}^{N} \left(\frac{g_i}{h_i}\right)^2 \qquad ?$$

die Frage wurde 1926 von E. Artin positiv beantwortet.

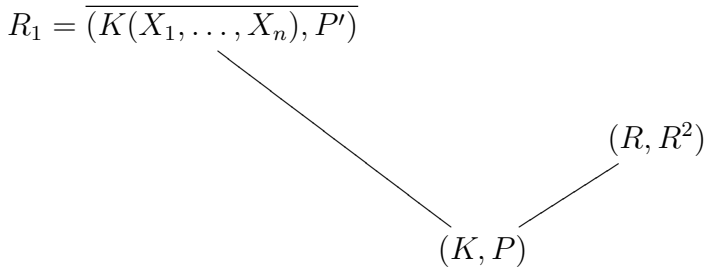
Satz 2.18. *Sei (K, P) ein angeordneter Körper, und sei (R, R^2) ein reell abgeschlossener Oberkörper von K mit $R^2 \cap K = P$ (z.B. der reelle Abschluß von K bezüglich P). Ist $f \in K[X_1, \ldots, X_n]$ mit $f(a_1, \ldots, a_n) \geq_{R^2} 0$ für alle $a_1, \ldots, a_n \in R$, so gilt $f \in \sum P\big(K(X_1, \ldots, X_n)\big)^2$.*

Beweis. Nach Lemma 1.19 ist $T = \sum P\big(K(X_1, \ldots, X_n)\big)^2$ eine Präordnung von $K(X_1, \ldots, X_n)$, da $-1 \notin T$ (man fasse die die Elemente einfach als rationale Funktionen auf). Nach Satz 1.16 ist

$$T = \bigcap_{\substack{T \subseteq P' \\ P' \text{ Anordnung von} \\ K(X_1, \ldots, X_n)}} P' \qquad P' = \bigcap_{\substack{P \subseteq P' \\ P' \text{ Anordnung von} \\ K(X_1, \ldots, X_n)}} P'$$

.

Annahme: $f \notin T$. Dann ist $f \notin P'$ für *eine* solche Anordnung. D.h. $f <_{P'} 0$ in $\big(K(X_1, \ldots, X_n), P'\big)$.
Setze $R_1 := \overline{\big(K(X_1, \ldots, X_n), P'\big)}$ und $R_2 := R$. Es gilt $R_1^2 \cap K = P$, sowie $R_2^2 \cap K = P$.



Betrachte nun die über (K, P) semialgebraische Mengen
$S(R_1) = \{x \in R_1^n \mid f(x_1, \ldots, x_n) <_{R_1^2} 0\} \subseteq R_1^n$ und
$S(R_2) = \{x \in R_2^n \mid f(x_1, \ldots, x_n) <_{R_2^2} 0\} \subseteq R_2^n$.
Nun ist aber $(X_1, \ldots, X_n) \in S(R_1)$, d.h. $S(R_1) \neq \emptyset$. Mit Korollar 2.17 folgt $S(R) = S(R_2) \neq \emptyset$, d.h. es gibt $(a_1, \ldots, a_n) \in R^n$ mit $f(a_1, \ldots, a_n) <_{R^2} 0$. Widerspruch! $\square$

2.4.2 Anwendungsbeispiel: Satz von Artin-Lang

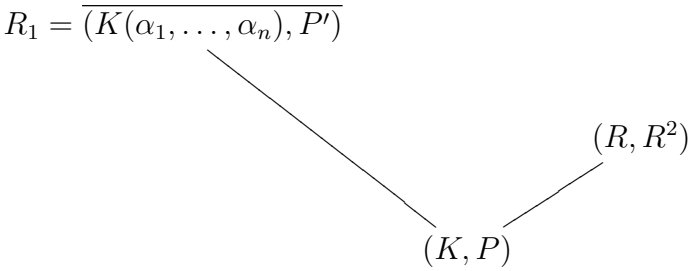
Satz 2.19. *Seien (K, P) ein angeordneter Körper und $\Big(K(\alpha_1, \ldots, \alpha_n), P'\Big)$ eine endlich erzeugte Körpererweiterung mit $P' \cap K = P$. Weiter seien $f_i(\alpha) \in K[\alpha_1, \ldots, \alpha_n]$ $(1 \leq i \leq m)$ mit $f_i(\alpha) >_{P'} 0$. Dann gibt es einen Homomorphismus $\varphi\colon K[\alpha_1, \ldots, \alpha_n] \longrightarrow R$ mit $\varphi|_K = \mathrm{id}$ und $\varphi(f_i(\alpha)) >_{R^2} 0$ für $1 \leq i \leq m$, wobei $R = \overline{\big(K, P\big)}$ ist.*

Beweis. Sei $I = \{g \in K[X_1, \ldots, X_n] \mid g(\alpha_1, \ldots, \alpha_n) = 0\}$.
I ist ein Ideal in $K[X_1, \ldots, X_n] = K[X]$. Mit dem Hilbertschen Basissatz folgt

$$I = g_1 K[X] + \cdots + g_r K[X] = (g_1, \ldots, g_r)_{K[X]}$$

für gewisse $g_1, \ldots, g_r \in K[X]$.
Betrachte nun die über K semialgebraische Menge

$$S = \left\{ (x_1, \ldots, x_n) \mid \bigwedge_{i=1}^{r} g_i(x) = 0 \wedge \bigwedge_{j=1}^{m} f_j(x) > 0 \right\}.$$



Im reellen Abschluss R_1 von $(K(\alpha_1, \ldots, \alpha_n), P')$ ist diese Menge nicht leer, da $(\alpha_1, \ldots, \alpha_n) \in S(R_1)$.

Also gibt es auch $a_1, \ldots, a_n \in R$ mit $g_i(a_1, \ldots, a_n) = 0$ für $1 \leq i \leq r$ und $f_j(a_1, \ldots, a_n) > 0$ für $1 \leq j \leq m$. Dann definiert

$$\begin{aligned} \varphi\colon K[\alpha_1, \ldots, \alpha_n] &\longrightarrow R \\ h(\alpha_1, \ldots, \alpha_n) &\mapsto h(a_1, \ldots, a_n) \end{aligned}$$

aber einen Homomorphismus mit $\varphi|_K = \mathrm{id}$ und $\varphi(f_j) > 0$ für $1 \leq j \leq m$. Für die Wohldefiniertheit ist dabei nur

$$h(\alpha) = 0 \implies h(a) = 0 \quad \text{für alle } h \in K[X]$$

zu zeigen. Es gilt nun

$$\begin{aligned} h(\alpha) = 0 &\implies h \in I \\ &\implies h = p_1 g_1 + \cdots + p_r g_r \quad \text{für gewisse } p_i \in K[X]. \end{aligned}$$

Also ist $h(a) = p_1(a)g_1(a) + \cdots + p_r(a)g_r(a) = 0$, da alle $g_j(a) = 0$. □

Definition 2.20. Sei A ein Ring. Ein *semialgebraischer Ausdruck* $\Phi(X_1, \ldots, X_n)$ in $X_1, \ldots, X_n$ über A ist eine boolsche Kombination mit $\wedge, \vee$ und $\neg$ von Ausdrücken der Gestalt $g = 0$ und $f > 0$, wobei $f, g \in A[X_1, \ldots, X_n]$ sind.

Beachte: Über jedem angeordneten Körper $(K, \leq)$ mit $A \subseteq K$ ist jeder semialgebraische Ausdruck äquivalent zu einem Ausdruck in "Normalform":

$$\bigvee_{i=1}^{r} \left(g_i = 0 \wedge \bigwedge_{j=1}^{s_i} f_{i,j} > 0 \right).$$

Definition 2.21. Ein (pränexer) *Ausdruck* über A in $X_1, \ldots, X_n$ hat die Gestalt

$$Q_1 Y_1 \quad Q_2 Y_2 \ \cdots \ Q_m Y_m \quad \Phi(X_1, \ldots, X_n, Y_1, \ldots, Y_m),$$

wobei $\Phi(X_1, \ldots, Y_m)$ ein semialgebraischer Ausdruck in $X_1, \ldots, Y_m$ über A und jedes Q_i entweder ein Existenzquantor $\exists$ oder ein Allquantor $\forall$ ist.

Satz 2.22 (Quantorenelimination). *Zu jedem pränexen Ausdruck*

$$Q_1 Y_1 \ldots Q_m Y_m \quad \Phi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$$

über $\mathbb{Z}$ gibt es einen semialgebraischen Ausdruck $\psi(X_1, \ldots, X_n)$ über $\mathbb{Z}$, so dass für jeden reell abgeschlossenen Körper R und für alle $a_1, \ldots, a_n \in R$ gilt:

$$(Q_1 b_1 \in R) \ldots (Q_m b_m \in R)\, \Phi(a_1, \ldots, a_n, b_1, \ldots, b_m) \iff \psi(a_1, \ldots, a_n).$$

Beweis. Induktion über $m \geq 0$:
$\underline{m = 0}$: klar.
$\underline{m - 1 \to m}$: Nach Induktionsvoraussetzung finden wir einen semialgebraischen Ausdruck $\psi_1(X_1, \ldots, X_n, Y)$ über $\mathbb{Z}$, so dass für alle reell abgeschlossenen Körper R und alle Elemente $a \in R^n$ und $b_1 \in R$ gilt

$$(Q_2 b_2 \in R) \ldots (Q_m b_m \in R)\, \Phi(a, b_1, b_2, \ldots, b_m) \iff \psi_1(a, b_1).$$

Also gilt für alle reell abgeschlossenen Körper und alle $a \in R^n$

$$(Q_1 b_1 \in R) \dots (Q_m b_m \in R)\, \Phi(a,b) \iff (Q_1 b_1 \in R)\, \psi_1(a,b_1).$$

1. Fall: $Q_1 = \exists$
Mit dem Projektionssatz erhalten wir einen semialgebraischen Ausdruck $\psi(X_1,\dots,X_n)$ über $\mathbb{Z}$, so dass für alle reell abgeschlossenen Körper R und alle $a \in R^n$ gilt

$$\exists b_1 \in R\, \psi_1(a,b_1) \iff \psi(a).$$

2. Fall: $Q_1 = \forall$
Wegen $(\forall b_1 \in R)\, \psi_1(a,b_1) \iff \neg\exists b_1 \in R\, \neg\psi_1(a,b_1)$ können wir auf die rechte Seite den ersten Fall anwenden. □

Satz 2.23 (Tarskis Transferprinzip). *Seien R_1, R_2 zwei reell abgeschlossene Körper über einem gemeinsamen Körper K, auf dem sie die gleiche Anordnung induzieren. Weiter sei $\psi(X_1,\dots,X_n)$ ein pränexer Ausdruck in $X_1,\dots,X_n$ über K. Dann gilt für alle $a_1,\dots,a_n \in K$:*

$$\psi(a_1,\dots,a_n) \text{ gilt in } R_1 \quad\iff\quad \psi(a_1,\dots,a_n) \text{ gilt in } R_2.$$

Beweis. Ersetze zunächst die Konstanten $c_1,\dots,c_s$ in ψ durch Unbestimmte $Z_1,\dots,Z_s$. Dann ist $\psi(X_1,\dots,X_n,Z_1,\dots,Z_s)$ ein pränexer Ausdruck über $\mathbb{Z}$. Mit Satz 2.22 gibt es dazu einen semialgebraischen Ausdruck Φ über $\mathbb{Z}$ in $X_1,\dots,X_n,Z_1,\dots,Z_s$, so dass für alle reell abgeschlossenen Körper R und alle $a_1,\dots,a_n,c_1,\dots,c_s \in R$ gilt

$$\psi(a_1,\dots,a_n,c_1,\dots,c_s) \iff \Phi(a_1,\dots,a_n,c_1,\dots,c_s).$$

Also gilt für $a_1,\dots,a_n,c_1,\dots,c_s \in K$

$$\begin{aligned}
&\psi(a_1,\dots,a_n,c_1,\dots,c_s) \text{ gilt in } R_1\\
\Leftrightarrow\ &\Phi(a_1,\dots,a_n,c_1,\dots,c_s) \text{ gilt in } R_1\\
\Leftrightarrow\ &\Phi(a_1,\dots,a_n,c_1,\dots,c_s) \text{ gilt in } K\\
\Leftrightarrow\ &\Phi(a_1,\dots,a_n,c_1,\dots,c_s) \text{ gilt in } R_2\\
\Leftrightarrow\ &\psi(a_1,\dots,a_n,c_1,\dots,c_s) \text{ gilt in } R_2.
\end{aligned}$$

Dabei wurde verwendet, dass ein semialgebraischer Ausdruck über K für gewisse Elemente aus K in R_1 bzw. R_2 genau dann gilt, wenn sie in K gilt (beachte: R_1 und R_2 induzieren nach Voraussetzung auf K die gleiche Anordnung). □

Beispiel 2.24 (zur Quantorenelimination). Sei $S = \{a \in R^n \mid \Phi(a)\}$ semialgebraisch über A (d.h. Φ ist ein semialgebraischer Ausdruck über A). Dann ist auch das Innere $\overset{\circ}{S}$ von S semialgebraisch über A. Denn es ist

$$\overset{\circ}{S} = \{a \in S \mid \text{ es gibt eine Kugel um } a, \text{ welche in } S \text{ liegt }\}.$$

Drückt man dies korrekt als pränexen Ausdruck aus, erhält man etwas wie das folgende:

$$\begin{aligned} a \in \overset{\circ}{S} &\iff \exists\epsilon\forall x_1,\ldots,x_n[\epsilon > 0 \wedge (\sum(x_i - a_i)^2 < \epsilon \rightarrow \Phi(x_1,\ldots,x_n))] \\ &\iff \exists\epsilon\forall x_1,\ldots,x_n[\epsilon > 0 \wedge (\Phi(x_1,\ldots,x_n) \vee \sum(x_i - a_i)^2 \geq \epsilon)]. \end{aligned}$$

Nach dem Satz über die Quantorenelimination ist $\overset{\circ}{S}$ also durch einen semialgebraischen Ausdruck beschreibbar.

Als Spezialfall erhalten wir aus Satz 2.23:

Korollar 2.25. *Ist ψ ein pränexer Ausdruck über $\mathbb{Z}$ ohne Variablen, der in $\mathbb{R}$ gilt, so gilt ψ auch in jedem reell abgeschlossenen Körper R.*

Beweis. Dies folgt unmittelbar aus Satz 2.23, wenn man beachtet, dass $\mathbb{Q}$ gemeinsamer Unterkörper von $\mathbb{R}$ und R ist.

□

3 Reelle Ringe

3.1 Das reelle Spektrum

Definition 3.1. Sei A ein kommutativer Ring mit $1 \neq 0$. $T \subset A$ heißt *Präpositivbereich* von A, falls

$$T + T \subseteq T, \quad T \cdot T \subseteq T, \quad A^2 \subseteq T, \quad -1 \notin T.$$

$T \cap -T =: \operatorname{supp} T$ heißt *Support* von T.
T heißt *Positivbereich*, falls $\operatorname{supp} T$ ein Primideal von A ist und $T \cup -T = A$ gilt.

Behauptung 3.2. *Sei T ein Präpositivbereich. Dann gilt*

$$T \cup -T = A \Longrightarrow T \cap -T \text{ ist ein Ideal.}$$

Beweis. Die additive Abgeschlossenheit von $T \cap -T$ folgt unmittelbar aus der additiven Abgeschlossenheit von T.
Sei also $a \in A$. Dann gilt nach Voraussetzung $a \in T$ oder $a \in -T$. Aus der multiplikativen Abgeschossenheit von T folgt dann aber sofort $a(T \cap -T) \subseteq (T \cap -T)$. □

Lemma 3.3. *Sei T ein Präpositivbereich von A und $a, b \in A$. Falls $ab \in -T$, so ist $T + aT$ oder $T + bT$ wieder ein Präpositivbereich.*

Beweis. Sind $T + aT$ und $T + bT$ beides keine Präpositivbereiche, so folgt

$$-1 \in T + aT \text{ und } -1 \in T + bT,$$

also $-1 = t_1 + at_2$ und $-1 = t_1' + bt_2'$ für gewisse $t_i, t_i' \in T$. Daraus folgt

$$(1 + t_1)(1 + t_1') = abt_2t_2'$$

und also

$$-1 = t_1 + t_1' + t_1t_1' - abt_2t_2' \in T,$$

Widerspruch. □

Satz 3.4. *Ist P ein maximaler Präpositivbereich, so ist P ein Positivbereich.*

Beweis. Zunächst ist $P \cup -P = A$ zu zeigen.
Sei dazu $a \in A$. Setze in Lemma 3.3 $b = -a$. Wegen $ab = -a^2 \in -P$ ist also $P + aP$ oder $P - aP$ ein Präpositivbereich, welcher P natürlich enthält. Aus der Maximalität von P folgt dann aber die Gleichheit, also gilt $a \in P$ oder $-a \in P$.
Damit ist aber $\operatorname{supp} P$ nach Behauptung 3.2 schon ein Ideal. Es bleibt also zu zeigen dass $\operatorname{supp} P$ prim ist.
Es gilt $-1 \notin P$, also $1 \notin \operatorname{supp} P$, also $\operatorname{supp} P \neq A$.
Sei nun $ab \in \operatorname{supp} P$ für gewisse $a, b \in A$ und $a \notin \operatorname{supp} P$.
Falls $a \notin P$, so kann $P + aP$ wegen der Maximalität von P kein Präpositivbereich mehr sein. Also ist $P + bP$ ein Präpositivbereich, da $ab \in -P$ (vgl. Lemma 3.3). Analog folgt aus $a(-b) \in -P$ auch, dass $P - bP$ ein Präpositivbereich sein muss. Also ist $P = P + bP = P - bP$, wiederum wegen der Maximalität von P. Somit folgt $b \in P$ und $-b \in P$, also $b \in \operatorname{supp} P$.
Falls $-a \notin P$, so ist $P - aP$ kein Präpositivbereich. Dann folgt gleich wie im ersten Fall $b \in P$ und $-b \in P$, also auch $b \in \operatorname{supp} P$.
Damit ist $\operatorname{supp} P$ ein Primideal. □

Korollar 3.5. *Jeder Präpositivbereich T ist in einem Positivbereich enthalten.*

Beweis. Man wähle mit dem Zorn'schen Lemma einen maximalen Präpositivbereich über T und verwende Satz 3.4. □

Wir zeigen nun einige Eigenschaften von Positivbereichen auf Ringen.

Behauptung 3.6. *Seien P, P' und P'' Positivbereiche von A. Dann gilt:*

(1) $P \subseteq P' \Longrightarrow \operatorname{supp} P \subseteq \operatorname{supp} P'$

(2) $P \subseteq P'$ *und* $\operatorname{supp} P = \operatorname{supp} P' \Longrightarrow P = P'$

(3) $P \subseteq P'$ *und* $P \subseteq P'' \Longrightarrow P' \subseteq P''$ *oder* $P'' \subseteq P'$.

(4) Sei $\varphi\colon A \longrightarrow B$ ein Ringhomomorphismus und $P \subseteq B$ ein Positivbereich. Dann ist $P' := \varphi^{-1}(P)$ ein Positivbereich von A mit $\operatorname{supp} P' = \varphi^{-1}(\operatorname{supp} P)$.

Beweis. (1): Klar.
(2): Sei $a \in P'$ und $a \notin P$. Dann ist $-a \in P \subseteq P'$, also $a \in \operatorname{supp} P' = \operatorname{supp} P \subseteq P$, Widerspruch.

(3): Angenommen es gibt $a \in P' \setminus P''$ und $b \in P'' \setminus P'$. Dann kann $a - b$ nicht in P sein (sonst $a = (a-b)+b \in P''$), ebenso kann $b-a$ nicht in P sein (sonst $b = (b-a)+a \in P'$). Dies ist aber ein Widerspruch zu $P \cup -P = A$.
(4): Offensichtlich übertragen sich die erforderlichen Eigenschaften via φ von P auf P'. □

Sei nun P ein Positivbereich von A und bezeichne $\mathfrak{p} = P \cap -P$ den Support von P. Wir betrachten den kanonischen Homomorphimus

$$\alpha_P \colon A \twoheadrightarrow A/\mathfrak{p} =: \overline{A}$$

und bezeichnen mit $\overline{P} := \{\overline{a} \mid a \in P\}$ das Bild von P unter α_P. Es ist $\overline{P} \subseteq \overline{A}$ und es gelten die folgenden Eigenschaften:

$$\overline{P} \dotplus \overline{P} \subseteq \overline{P}, \quad \overline{A}^2 \subseteq \overline{P}, \quad -\overline{1} \notin \overline{P}, \quad \overline{A} = \overline{P} \cup -\overline{P},$$

$$\overline{P} \cap -\overline{P} = \{0\} \text{ und } \alpha_P^{-1}(\overline{P}) = P.$$

Außerdem ist $\overline{A}$ ein Integritätsbereich ($\mathfrak{p}$ war ein Primideal). Sei $K := \operatorname{Quot} \overline{A}$ der Quotientenkörper von $\overline{A}$.

Behauptung 3.7. *$\overline{P}$ definiert einen Positivbereich P' auf K durch*

$$\frac{\overline{a}}{\overline{b}} \in P' :\Longleftrightarrow \overline{a}\overline{b} \in \overline{P}.$$

Es gilt $P' \cap \overline{A} = \overline{P}$.

Beweis. Zunächst ist die Wohldefiniertheit zu zeigen. Seien dazu

$$\frac{\overline{a}}{\overline{b}} = \frac{\overline{c}}{\overline{d}} \in K.$$

Dann gilt $\overline{a}\overline{d} = \overline{c}\overline{b}$, bzw. nach Multiplikation mit $\overline{b}\overline{d}$

$$\overline{a}\overline{b} \cdot \overline{d}^2 = \overline{c}\overline{d} \cdot \overline{b}^2.$$

Damit ist aber $\overline{a}\overline{b} \in \overline{P}$ genau dann, wenn $\overline{c}\overline{d} \in \overline{P}$, da aus $\overline{a}\overline{b} \in \overline{P}$ und $\overline{c}\overline{d} \notin \overline{P}$, also $\overline{c}\overline{d} \in -\overline{P} \setminus \{0\}$, folgt, dass $\overline{c}\overline{d} \cdot \overline{b}^2 = \overline{a}\overline{b} \cdot \overline{d}^2$ in $\overline{P} \cap -\overline{P} = \{0\}$ liegt, woraus sich aber der Widerspruch $\overline{c}\overline{d} = 0 \in \overline{P}$ ergibt.
Für $\frac{\overline{a}}{\overline{b}}, \frac{\overline{c}}{\overline{d}} \in P'$ gilt $\frac{\overline{a}}{\overline{b}} \cdot \frac{\overline{c}}{\overline{d}}$ und $\frac{\overline{a}}{\overline{b}} + \frac{\overline{c}}{\overline{d}} \in P'$, denn

$$\overline{a}\overline{b}\overline{c}\overline{d} \in \overline{P} \text{ und}$$

$$(\overline{a}\overline{d} + \overline{b}\overline{c})\overline{b}\overline{d} = \overline{a}\overline{b} \cdot \overline{d}^2 + \overline{c}\overline{d} \cdot \overline{b}^2 \in \overline{P}.$$

Wäre $-1 = \frac{-1}{1} \in P'$, so auch $-1 = (-1)1 \in \overline{P}$, Widerspruch.
$K^2 \subseteq P'$ und $P' \cup -P' = K$ ist klar.
Schließlich gilt

$$\frac{\overline{a}}{1} \in P' \Longleftrightarrow \overline{a} \in \overline{P},$$

also $P' \cap \overline{A} = \overline{P}$. □

Bemerkung 3.8. Ist P' ein Positivbereich von Quot A, so ist $P := P' \cap A$ ein Positivbereich von A mit supp $P = \{0\}$.

Beweis. Die Aussage folgt mit Behauptung 3.6 (4) aus der Tatsache, dass die Einbettung $i\colon A \hookrightarrow \text{Quot}\, A$ ein Homomorphismus mit $i^{-1}(\{0\}) = \{0\}$ ist (Beachte dabei dass jeder Körper natürlich auch ein Ring ist und der Begriff Positivbereich eines Rings dann übereinstimmt mit dem Begriff Positivbereich eines Körpers). □

Definition 3.9. Sper $A := \{P \subseteq A \mid P$ Positivbereich von A $\}$ heißt *reelles Spektrum von A*.

Beachte: Das *Spektrum* eines Ringes A ist definiert als

$$\text{Spec}\, A := \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ Primideal von A }\}.$$

Wir haben eine Abbildung

$$\begin{array}{ccc} \text{Sper}\, A & \longrightarrow & \text{Spec}\, A \\ P & \mapsto & P \cap -P. \end{array}$$

Beispiele 3.10. (1) Sei K ein Körper: Dann ist Spec $K = \{(0)\}$ und Sper K ist gerade die Menge der Körperanordnungen (vgl. Definition 1.11).
Es ist beispielsweise $\sharp\, \text{Sper}\, \mathbb{Q}(\sqrt{2}) = 2$ (dies folgt z.B. aus Korollar 1.39) und $\sharp\, \text{Sper}\, \mathbb{Q}(X) = \infty$.

(2) Sei $A = \mathbb{Z}$: Es ist Spec $\mathbb{Z} = \{p\mathbb{Z} \mid p$ Primzahl$\} \cup \{(0)\}$ und Sper $\mathbb{Z} = \{\mathbb{N}\}$. Denn außer dem von der (eindeutigen) Anordnung auf $\mathbb{Q}$ induzierten Positivbereich $\mathbb{N}$ kann es keine weiteren geben. Für ein Primideal der Form $p\mathbb{Z}$ mit p prim ist nämlich $\mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper, also kann es darauf keine Anordnung geben. Wegen Behauptung 3.7 gibt es

also auch keinen Positivbereich auf $\mathbb{Z}$ mit Support $p\mathbb{Z}$. Ebenso kann es keine weiteren Positivbereiche auf $\mathbb{Z}$ mit Support (0) geben, denn ein solcher müsste auch $\mathbb{N}$ enthalten, somit wären beide nach Behauptung 3.6 (2) schon gleich.

(3) Sei $A = \mathbb{R}[X]$: Es ist

$$\operatorname{Spec} \mathbb{R}[X] = \{(0), (X-a), ((X-a)^2 + b^2) \mid a, b \in \mathbb{R}, b \neq 0\}.$$

Sei $P \in \operatorname{Sper} \mathbb{R}[X]$. Es gibt nun mehrere Möglichkeiten:

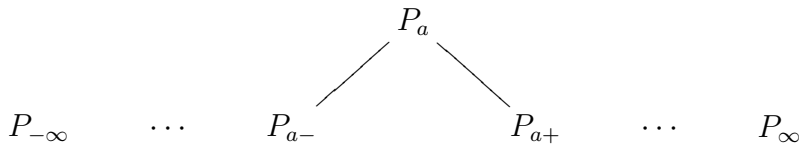
- $P \cap -P = (0)$. Dann ist $P = P' \cap \mathbb{R}[X]$ für eine Anordnung P' auf $\mathbb{R}(X)$ (folgt aus Behauptung 3.7).
- $P \cap -P = (X-a)$ für ein $a \in \mathbb{R}$. Betrachte die kanonische Projektion
$$\alpha_P \colon \mathbb{R}[X] \longrightarrow \mathbb{R}[X]/(X-a) \cong \mathbb{R}.$$
Es gilt mit Behauptung 3.6 (2) und (4) $P = \alpha_P^{-1}(\mathbb{R}^2)$ und wegen $\alpha_P(f(X)) = f(\alpha_P(X)) = f(a)$ ist also
$$P = \{f \in \mathbb{R}[X] \mid \alpha_P(f) \geq_{\mathbb{R}} 0\} = \{f \in \mathbb{R}[X] \mid f(a) \geq_{\mathbb{R}} 0\}.$$
Weiter ist $\operatorname{supp} P = \{f \in \mathbb{R}[X] \mid f(a) = 0\}$.
- $P \cap -P = ((X-a)^2 + b^2)$ für $a, b \in \mathbb{R}, b \neq 0$. Dann besitzt $\mathbb{R}[X]/\operatorname{supp} P = \mathbb{C}$ keine Anordnung, also kann es auch keinen solchen Positivbereich P auf $\mathbb{R}[X]$ gegeben haben.

Wir haben also insgesamt die folgende Situation: Für jedes $a \in \mathbb{R}$ bekommen wir drei verschiedene Positivbereiche auf $\mathbb{R}[X]$:

- Einen Positivbereich P_a, welcher durch den Einsetzungshomomorphismus von a induziert wird. Er hat das Primideal $(X-a)$ als Support.
- Einen Positivbereich P_{a+}, bei welchem das Element X unendlich nahe rechts neben dem Element a seine Position hat. Dieser Positivbereich kommt gerade von der entsprechenden Anordnung auf $\mathbb{R}(X)$ und hat Support (0).
- Einen Positivbereich P_{a-}, bei welchem das Element X seine Position unendlich nahe links neben dem Element a hat. Auch dieser Positivbereich kommt von $\mathbb{R}(X)$ und hat Support (0).

Zusätzlich gibt es noch die beiden Anordnungen auf $\mathbb{R}(X)$, bei welchen das Element X größer bzw. kleiner als alle reellen Zahlen ist. Auch diese induzieren natürlich Positivbereiche auf $\mathbb{R}[X]$, welche wir mit P_∞ und $P_{-\infty}$ bezeichnen. Insgesamt erhalten wir so alle Positivbereiche von $\mathbb{R}[X]$.

Es gelten die folgenden Inklusionen zwischen den verschiedenen Positivbereichen:



Definiert man $\operatorname{Sper}^{\max} A := \{P \in \operatorname{Sper} A \mid P \text{ maximal}\}$, so gilt

$$\operatorname{Sper}^{\max} \mathbb{R}[X] = \{P_{-\infty}, P_\infty\} \cup \{P_a \mid a \in \mathbb{R}\}.$$

(4) Sei $A = \mathbb{R}[X_1, \ldots, X_n]$. Hier gibt es gewisse "Extremfälle" von Positivbereichen P:

- $\operatorname{supp} P = (0)$: P kommt von einer Anordnung auf $\mathbb{R}(X_1 \ldots, X_n)$.
- $\operatorname{supp} P = (X_1 - a_1, \ldots, X_n - a_n)$ (mit $a_1, \ldots, a_n \in \mathbb{R}$) maximales Ideal in $\mathbb{R}[X_1, \ldots, X_n]$. Dann ist

$$\begin{array}{rcl} \alpha_P \colon \mathbb{R}[X_1, \ldots, X_n] & \longrightarrow & \mathbb{R} \cong \mathbb{R}[X_1, \ldots, X_n]/\operatorname{supp} P \\ f & \mapsto & f(a_1, \ldots, a_n), \end{array}$$

  d.h. der Positivbereich kommt von dem Punkt $(a_1, \ldots, a_n) \in \mathbb{R}^n$. Es gibt allerdings noch weitere Anordnungen auf $\mathbb{R}[X_1, \ldots, X_n]$.

3.2 Die spektrale Topologie

Sei wieder A ein kommutativer Ring mit $1 \neq 0$.

Definition 3.11. A heißt *semi-reell*, falls $-1 \notin \sum A^2$.

Bemerkung 3.12. A ist semi-reell $\iff \operatorname{Sper} A \neq \emptyset$.

Beweis. "⇒": Falls $-1 \notin \sum A^2$, so ist $\sum A^2$ ein Präpositivbereich. Dann folgt die Behauptung mit Korollar 3.5.
"⇐": Falls es einen Positivbereich auf A gibt, so ist $\sum A^2$ darin enthalten, und deshalb kann -1 keine Quadratsumme sein. □

Definition 3.13. A heißt *reell*, falls es einen Positivbereich P mit $\operatorname{supp} P = (0)$ auf A gibt.

Bemerkung 3.14. Ist A reell, so ist A ein Integritätsbereich und es gibt eine Anordnung auf $\operatorname{Quot} A$. Also gilt für $a_1, \ldots, a_n \in A$:

$$\sum_{i=1}^{n} a_i^2 = 0 \Longrightarrow a_i = 0 \text{ für alle } i.$$

Definition 3.15. Die *spektrale Topologie* auf $X = \operatorname{Sper} A$ ist diejenige Topologie, die von den Mengen der Gestalt

$$U(a) := \{P \in X \mid \alpha_P(a) > 0\} = \{P \in X \mid a \notin -P\}$$

für $a \in A$ erzeugt wird. Eine offene Menge der spektralen Topologie ist also eine beliebige Vereinigung von endlichen Durchschnitten solcher Mengen $U(a)$.

Definition 3.16. Die *konstruktible Topologie* auf $X = \operatorname{Sper} A$ ist diejenige Topologie, die von den Mengen $U(a)$ und deren Komplementen

$$X \setminus U(a) = \{P \in X \mid \alpha_P(a) \leq 0\} = \{P \in X \mid a \in -P\}$$

erzeugt wird.

Satz 3.17. *$X = \operatorname{Sper} A$ ist quasikompakt sowohl mit der konstruktiblen als auch mit der spektralen Topologie (dabei bedeutet quasi-kompakt, dass jede offene Überdeckung von X eine endliche Teilüberdeckung besitzt).*

Beweis. Wir identifizieren eine Teilmenge M von A mit ihrer charakteristischen Funktion

$$\chi_M(a) := \begin{cases} 0 \text{ falls } a \notin M \\ 1 \text{ falls } a \in M. \end{cases}$$

So können wir M auffassen als Element in

$$\{0,1\}^A = \{f \colon A \longrightarrow \{0,1\}\}.$$

$\{0,1\}^A$ ist aber nach dem Satz von Tychonoff (siehe Aufgabe 8.2) quasikompakt in der Produkttopologie (wobei auf $\{0,1\}$ die diskrete Topologie verwendet wird).

Die Produkttopologie ist aber gerade die gröbste Topologie, die alle Projektionen auf die einzelnen Komponenten stetig macht. Eine Projektion auf eine Komponente ist in unserem Fall aber gerade Einsetzen eines Elementes a aus A (wenn man die Elemente von $\{0,1\}^A$ wieder als Abbildungen auffasst). Also wird die Produkttopologie gerade von Mengen der Gestalt

$$O(a) = \{M \subseteq A \mid a \in M\} \text{ und } \{0,1\}^A \setminus O(a) = \{M \subseteq A \mid a \notin M\}$$

mit $a \in A$ erzeugt.

Eingeschränkt auf $X = \operatorname{Sper} A$ (welches man natürlich als eine Teilmenge von $\{0,1\}^A$ auffassen kann) sind dies aber gerade die Mengen die die konstruktible Topologie erzeugen. Also ist die Spurtopologie auf X gerade die konstuktible Topologie. Wenn wir nun also zeigen, dass X abgeschlossen in $\{0,1\}^A$ ist, folgt die Quasikompaktheit von X in der konstruktiblen Topologie (siehe Aufgabe 8.1 b)). Da die spektrale Topologie gröber ist, folgt daraus dann sofort auch die Quasikompaktheit in dieser Topologie.

Sei also $M \subseteq A$ mit $M \notin X$, d.h. M ist kein Positivbereich. Wir müssen zeigen, dass es eine offene Menge in $\{0,1\}^A$ gibt, welche M enthält und disjunkt zu X ist.

Es gibt nun verschiedene Möglichkeiten, warum M kein Positivbereich ist. Zum Beispiel könnte es $a, b \in M$ geben mit $a + b \notin M$. Dann ist aber offensichtlich die Menge

$$O(a) \cap O(b) \cap \big(\{0,1\}^A \setminus O(a+b)\big)$$

offen in $\{0,1\}^A$, sie enthält M und natürlich keine Anordnung.

Eine andere Möglich wäre, dass $-1 \in M$ gilt. Dann erfüllt aber die offene Menge $O(-1)$ die erwünschte Bedingung.

Analog läßt sich für jede andere Möglichkeit, warum M kein Positivbereich ist, eine passende offene Menge finden. Damit ist die Behauptung gezeigt. □

Definition 3.18. Sei $T \subseteq A$ ein Präpositivbereich. Wir definieren

$$\operatorname{Sper}_T A := \{P \in \operatorname{Sper} A \mid T \subseteq P\}.$$

Behauptung 3.19. $\operatorname{Sper}_T A$ *ist abgeschlossen in* $\operatorname{Sper} A$ *versehen mit der spektralen Topologie, also auch quasi-kompakt.*

Beweis. Ist $P \in \operatorname{Sper} A \setminus \operatorname{Sper}_T A$, so gibt es ein $t \in T$ mit $t \notin P$. Dann ist aber $U(-t)$ (siehe Definition 3.15) eine spektral-offene Menge in $\operatorname{Sper} A$, welche P enthält und disjunkt zu $\operatorname{Sper}_T A$ ist. □

Behauptung 3.20. $\operatorname{Sper}_T^{\max} A := \{P \in \operatorname{Sper}_T A \mid P \text{ maximal}\}$ *ist quasikompakt in der spektralen Topologie.*

Beweis. Sei $\bigcup_{i\in I} U_i$ eine spektral-offene Überdeckung von $\operatorname{Sper}_T^{\max}$ in $\operatorname{Sper} A$. Ohne Einschränkung ist dabei jedes U_i von der Gestalt

$$U_i = U(a_{i_1}) \cap \cdots \cap U(a_{i_{n_i}}),$$

denn so sehen Basismengen der spektralen Topologie aus.

Sei nun $Q \in \operatorname{Sper}_T A$ beliebig und $Q \subseteq P$ für ein $P \in \operatorname{Sper}_T^{\max}$. Dann ist $P \in U_i$ für ein $i \in I$ und also $\alpha_P(a_{i_j}) > 0$ für $j = 1, \ldots, n_i$.

Dies bedeutet aber $a_{i_j} \notin -P$ für $j = 1, \ldots, n_i$. Wegen $Q \subseteq P$ gilt also auch $a_{i_j} \notin -Q$ für $j = 1, \ldots, n_i$, was wiederum äquivalent zu $Q \in U_i$ ist.

Also ist $\bigcup_{i\in I} U_i$ sogar schon eine spektral-offene Überdeckung von $\operatorname{Sper}_T A$. Mit Behauptung 3.19 gibt es dann aber eine endliche Teilüberdeckung von $\operatorname{Sper}_T A$, welche natürlich auch eine endliche Teilüberdeckung von $\operatorname{Sper}_T^{\max}$ ist. □

Behauptung 3.21. $\operatorname{Sper}_T^{\max} A$ *ist haussdorffsch in der spektralen Topologie.*

Beweis. In Aufgabe 8.3 c) soll dies für $\operatorname{Sper}^{\max} A$ gezeigt werden. Der Beweis hier geht analog. □

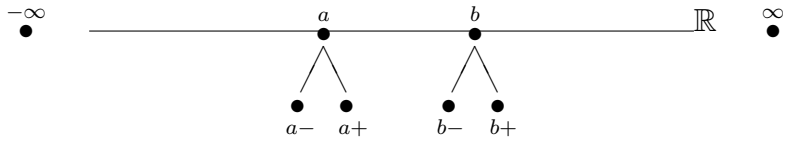
Beispiel 3.22. Wir untersuchen die spektrale Topologie auf $\operatorname{Sper} \mathbb{R}[X]$ (zu $\operatorname{Sper} \mathbb{R}[X]$ siehe Beispiele 3.10 (3)). Genauer interessieren uns die Mengen $U(f)$ mit $f \in \mathbb{R}[X]$. Im Beweis von Behauptung 3.20 haben wir gesehen, dass eine Menge $U(f)$ mit einem Positivbereich P auch alle kleineren Positivbereiche $Q \subseteq P$ enthält.

Ist in unserem Fall also $P_a \in U(f)$ für ein $a \in \mathbb{R}$, so auch $P_{a-}, P_{a+} \in U(f)$ (vergleiche Bild auf Seite 46).

Umgekehrt gibt es aber Mengen $U(f)$, die beispielsweise ein P_{a+} enthalten, aber nicht P_a. Betrachten wir etwa

$$f = -(X - a)(X - b)$$

für $a, b \in \mathbb{R}$ mit $a < b$.



Offensichtlich ist $P_a \notin U(f)$, da $\alpha_{P_a}(f) = f(a) = 0$ gilt. Ebenso ist $P_{a-} \notin U(f)$, da $(X-a) <_{P_{a-}} 0, (X-b) <_{P_{a-}} 0$ und somit $f <_{P_{a-}} 0$ gilt. Allerdings sieht man auf gleiche Weise dass $f >_{P_{a+}} 0$ gilt, also $P_{a+} \in U(f)$. Ebenso erhält man $P_b, P_{b+} \notin U(f)$, aber $P_{b-} \in U(f)$. Für $a < c < b$ ist offensichtlich $f(c) > 0$, also ist $P_c \in U(f)$. Letztendlich ist $f \notin P_{\pm\infty}$. Somit ist

$$U(f) = \{P_{a+}, P_{b-}\} \cup \{P_{c-}, P_c, P_{c+} \mid a < c < b\}.$$

Für

$$f = X - a$$

mit $a \in \mathbb{R}$ sieht man auf gleiche Weise wie oben

$$U(f) = \{P_{a+}, P_\infty\} \cup \{P_{c-}.P_c, P_{c+} \mid a < c\}.$$

3.3 Das reelle Spektrum von $\mathbb{R}[X_1, \ldots, X_n]$

Sei $A = R[X_1, \ldots, X_n]$ mit R reell abgeschlossener Körper. Weiter sei $K = R(X_1, \ldots, X_n)$ der Quotientenkörper von A. Das reelle Spektrum

$$X_K = \operatorname{Sper} K$$

besteht genau aus den Anordnungen (Positivbereichen) von K. Diese entsprechen umkehrbar eindeutig den Positivbereichen $P \in \operatorname{Sper} A$ mit $P \cap -P = \{0\}$. Wir wollen deshalb X_K als Teilraum von $\operatorname{Sper} A$ verstehen. Genauer gilt (wie man sofort sieht)

$$X_K \subseteq \operatorname{Sper}^{\min} A \subseteq \operatorname{Sper} A.$$

Ordnen wir jedem Punkt $a = (a_1, \ldots, a_n) \in R^n$ den Positivbereich

$$P_a = \{f \in A \mid f(a) \geq 0\}$$

zu und beachten wir, dass

$$\operatorname{supp} P_a = \{f \in A \mid f(a) = 0\}$$

das maximale Ideal $(x_1 - a_1, \ldots, x_n - a_n)$ in A ist, so erkennen wir mit 3.6(2), dass $P_a \in \operatorname{Sper}^{max} A$. Identifizieren wir dann a mit P_a, so erhalten wir die Inklusion

$$R^n \subseteq \operatorname{Sper}^{\max} A \subseteq \operatorname{Sper} A.$$

Eine kleine Überlegung zeigt, dass die spektrale Topologie von $\operatorname{Sper} A$ auf R^n gerade die Produkttopologie der Intervalltopologie von R induziert. Dazu folgende

Definition 3.23. Wir ordnen jedem semialgebraischen Ausdruck $\sigma(X_1, \ldots, X_n)$ über R sowohl die semialgebraische Teilmenge

$$S_\sigma(R) = \{a \in R^n \mid \sigma(a) \text{ gilt in } R\}$$

von R^n als auch die konstruktible Teilmenge $\widetilde{S}_\sigma$ von $\operatorname{Sper} A$ zu. Dabei ist für den Ausdruck $f(X_1, \ldots, X_n) > 0$

$$\widetilde{S}_{f>0} = \{P \in \operatorname{Sper} A \mid \alpha_p(f) > 0\} = U(f)$$

und für eine boolsche Kombination σ von Ausdrücken der Gestalt $f > 0$ wird $\widetilde{S}_\sigma$ gemäß derselben booleschen Kombination gebildet. Also z.B. ist

$$\widetilde{S}_{f>0 \wedge \neg g>0} = \widetilde{S}_{f>0} \cap (\operatorname{Sper} A \smallsetminus \widetilde{S}_{g>0}).$$

Nun ist klar, dass folgendes gilt:

$$\widetilde{S_\sigma} \cap R^n = S_\sigma(R).$$

Damit sieht man die obige Behauptung über die induzierte Topologie ein.

Die Zuordnung $S_\sigma \longmapsto \widetilde{S}_\sigma$ für semialgebraische Mengen ist überaus nützlich. Wir werden nun den folgenden tiefliegenden Satz in Etappen beweisen.

Satz 3.24. *Seien R ein reell abgeschlossener Körper und $A = R[X_1, \ldots, X_n]$wie oben. Dann gilt für semialgebraische Ausdrücke $\sigma, \sigma_1, \sigma_2$ über R:*

(I) $S_\sigma(R) \neq \emptyset \Leftrightarrow \widetilde{S}_\sigma \neq \emptyset$

(II) $S_{\sigma_1}(R) = S_{\sigma_2}(R) \Leftrightarrow \widetilde{S_{\sigma_1}} = \widetilde{S}_{\sigma_2}$

(III) $S_\sigma(R)$ *offen in* $R^n \Leftrightarrow \widetilde{S}_\sigma$ *spektral offen in* $\operatorname{Sper} A$.

Sofort einsehbar sind die Richtungen (I) "$\Rightarrow$", (II) "$\Leftarrow$" und (III) "$\Leftarrow$".

Beweis. (I): Sei $P \in \operatorname{Sper} A$. Wir erinnern uns: Ist σ der Ausdruck $f(X_1, \ldots, X_n) > 0$, so bedeutet $P \in \widetilde{S}_\sigma$ gerade $0 < \alpha_P(f(X_1, \ldots, X_n)) = f(\alpha_P(X_1), \ldots, \alpha_P(X_n))$ bezüglich der Anordnung $\overline{P}$ von $\overline{A} = A/\operatorname{supp} P$. Für ein semialgebraisches $\sigma(X_1, \ldots, X_n)$ bedeutet $P \in \widetilde{S}_\sigma$ also, dass $\sigma(\alpha_P(X_1), \ldots, \alpha_P(X_n))$ in dem angeordneten Integritätsbereich $(\overline{A}, \overline{P})$ gilt. Dies ist äquivalent dazu, dass $\sigma(\alpha_P(X_1), \ldots, \alpha_P(X_n))$ in dem reellen Abschluss R' des Quotientenkörpers von $(\overline{A}, \overline{P})$ gilt. Insbesondere ist dann $S_\sigma(R') \neq \emptyset$. Da R gemeinsamer angeordneter Unterkörper von R' und R ist, folgt mit Korollar 2.17 daraus $S_\sigma(R) \neq \emptyset$. □

Korollar 3.25. *R^n ist bezüglich der konstruktiblen Topologie dicht in* $\operatorname{Sper} A$.

Beweis. Sei ohne Einschränkung $\widetilde{S}_\sigma$ eine konstruktibel (offene) Umgebung von P, also $P \in \widetilde{S}_\sigma$. Dann exisitert $a \in S_\sigma(R)$ und damit gilt $P_a \in \widetilde{S}_\sigma$. □

Beweis. (II): Es genügt zu zeigen:

$$S_{\sigma_1}(R) \subseteq S_{\sigma_2}(R) \Rightarrow \widetilde{S}_{\sigma_1} \subseteq \widetilde{S}_{\sigma_2}.$$

Dies folgt jedoch mit $\sigma \equiv (\sigma_1 \wedge \neg\sigma_2)$ sofort aus (I), da

$$S_\sigma(R) = \emptyset \Leftrightarrow S_{\sigma_1}(R) \subseteq S_{\sigma_2}(R),$$

und analog für $\widetilde{S}_\sigma$. □

Bevor wir in den etwas längeren Beweis von (III) eintreten, wollen wir ein interessantes Korollar hervorheben.

Ist $\widetilde{S}_\sigma$ spektral offen, so ist es (nach Definition) eine potentiell unendliche Vereinigung von Mengen der Gestalt

$$\widetilde{S}_{f_1>0\wedge\cdots\wedge f_m>0} = U(f_1) \cap \cdots \cap U(f_m)$$

mit $f_i \in R[X_1, \ldots, X_n]$. Da aber $\widetilde{S}_\sigma$ auch konstruktibel abgeschlossen ist, ist $\widetilde{S}_\sigma$ quasi-kompakt in der konstruktiblen Topologie von $\operatorname{Sper} A$. Es reichen also schon endlich viele der obigen Vereinigungsglieder aus, um $\widetilde{S}_\sigma$ zu erhalten. Also gilt

$$\widetilde{S}_\sigma = \bigcup_{i=1}^{r} \bigcap_{j=1}^{m_i} U(f_{ij}).$$

Schneidet man wieder mit R^n, so erhält man

Korollar 3.26. *(Endlichkeitssatz) Ist eine semialgebraische Teilmenge $S \subseteq R^n$ offen, so ist sie schon endliche Vereinigung von endlichen Durchschnitten $S_{f_1>0}(R) \cap \cdots \cap S_{f_m>0}(R)$.*

Die noch fehlende Implikation von Teil (III) des Satzes 3.24 folgern wir aus dem:

Spezialisierungssatz 3.27. *Ist $S_\sigma(R)$ abgeschlossen im R^n, so ist $\widetilde{S}_\sigma$ abgeschlossen unter Spezialisierungen in* $\operatorname{Sper} A$*, d.h. gilt für $P, P' \in \operatorname{Sper} A$, dass $P \subseteq P'$ und $P \in \widetilde{S}_\sigma$, so gilt auch $P' \in \widetilde{S}_\sigma$.*

Beweis. (III): Sei $S_\sigma(R)$ offen. Dann ist $\widetilde{S}_{\neg\sigma} = \operatorname{Sper} A \setminus \widetilde{S}_\sigma$ nach dem Spezialisierungssatz unter Spezialisierungen abgeschlossen. Wir fixieren $P' \in \widetilde{S}_\sigma$.

Zu jedem $P \in \widetilde{S}_{\neg\sigma}$ gibt es dann ein $f_P \in P$, das nicht in P' liegt. Damit liefern die konstruktibel offenen Mengen

$$\widetilde{S}_{f_P \geq 0} \quad \text{mit} \quad P \in \widetilde{S}_{\neg\sigma}$$

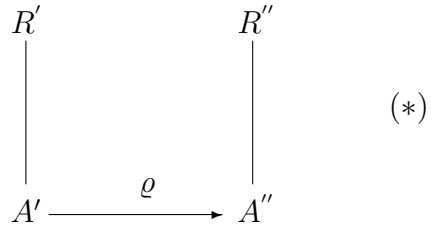
eine Überdeckung (die nicht P' enthält) der konstruktibel kompakten Menge $\widetilde{S}_{\neg\sigma}$. Also reichen schon endlich viele zur Überdeckung. Damit erhalten wir $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$ mit

$$P' \in \widetilde{S}_{-f_1>0} \cap \cdots \cap \widetilde{S}_{-f_m>0} \subseteq \widetilde{S}_\sigma.$$

Also gibt es zu jedem $P' \in \widetilde{S}_\sigma$ eine spektral offene Umgebung in $\widetilde{S}_\sigma$, d.h. $\widetilde{S}_\sigma$ ist spektral offen. □

Beweis. (Spezialisierungssatz): Es seien $S_\sigma(R)$ abgeschlossen und $P', P'' \in \operatorname{Sper} A$ mit $P' \subseteq P''$ und $P' \in \widetilde{S}_\sigma$. Also gilt $\sigma(x_1', \ldots, x_n')$ in $A' = A/\operatorname{supp} P'$ bzgl. der Anordnung $P'/\operatorname{supp} P'$, wobei $x_i' = \alpha_{P'}'(X_i)$ ist. Wir müssen zeigen, dass $\sigma(x_1'', \ldots, x_n'')$ in $A'' = A/\operatorname{supp} P''$ bzgl. der Anordnung $P''/\operatorname{supp} P''$ gilt, wobei $x_i'' = \alpha_{p''}(X_i)$ ist. Es sei R' der reelle Abschluss des Quotientenkörpers von A' bzgl. der durch P' induzierten Anordnung. Analog sei R'' der reelle Abschluss von $\operatorname{Quot}(A'')$ bzgl. P''.

Wir erhalten dann die folgende Situation:



Hierbei ist, wegen $P' \subseteq P''$ (und deswegen $\operatorname{supp} P' \subseteq \operatorname{supp} P''$), die Abbildung definiert durch $\varrho|_R = \mathrm{id}$ und $\varrho(x_i') = x_i''$ ein ordnungstreuer R-Algebren-Homomorphismus, d.h. es gilt für $a, b \in A'$

$$a \leq' b \Rightarrow \varrho(a) \leq'' \varrho(b).$$

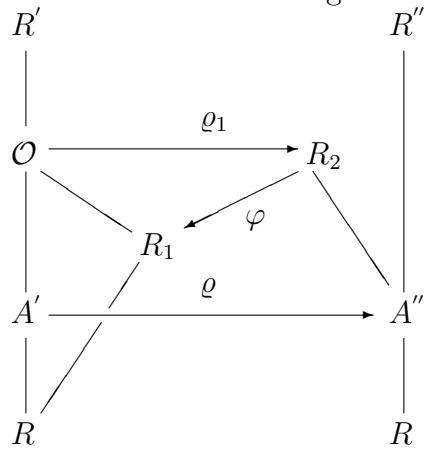
Dabei bezeichnen $\leq'$ und $\leq''$ die Anordnungen von R' bzw. R''.

Wir verwenden dann die beiden folgenden Hilfssätze, deren Beweis wir vorerst zurückstellen.

Hilfssatz 3.28. *Es sei ein Diagramm* $(*)$ *gegeben, wobei* R', R'' *reell abgeschlossene Körper,* A', A'' *Unterringe und* ϱ *ein surjektiver ordnungstreuer Ringhomomorphismus sind. Dann lässt sich* ϱ *auf einen konvexen Unterring* $\mathcal{O}$ *von* R' *zu* ϱ_1 *ordnungstreu so fortsetzen, dass* $\varrho_1 \colon \mathcal{O} \twoheadrightarrow R_2$. *wobei* $A'' \subseteq R_2$ *und* R_2 *reell abgeschlossen sind.*

Hilfssatz 3.29. *Sind* R' *und* R_2 *reell abgeschlossen,* $\mathcal{O}$ *ein konvexer Teilring von* R' *und* $\varrho_1 : \mathcal{O} \twoheadrightarrow R_2$ *ein ordnungstreuer Ringhomomorphismus, so existiert ein Schnitt* $\varphi \colon R_2 \to \mathcal{O}$ *für* ϱ_1, *d.h.* φ *ist ein Homomorphismus mit* $\varrho_1 \circ \varphi = \mathrm{id}$.

Unter Benutzung der Hilfssätze erhalten wir folgendes erweiterte Diagramm:



Dabei ist $R_1 := \varphi(R_2)$. Alle Homomorphismen ϱ, ϱ_1 und φ sind auf R die Identität, und sie sind ordnungstreu bzgl. der Ordnungen $\leq^{'}$ und $\leq^{''}$.

Nimmt man nun an, dass $\sigma(x^{''})$ in $A^{''}$ und damit auch in R_2 nicht gilt, so gilt $\sigma(\varphi(x^{''}))$ nicht in R_1. Mit Tarskis Transferprinzip 2.23 folgt aber, dass die Menge

$$\{z \in R_1^n \mid \sigma(z) \text{ gilt in } R_1\}$$

abgeschlossen im R_1^n ist (da die entsprechende Menge im R^n abgeschlossen ist und diese Tatsache sich durch einen pränexen Ausdruck ψ ohne Variablen aber mit Parametern in R ausdrücken lässt). Also gibt es ein $0 < \varepsilon \in R_1$, so dass in R_1 gilt:

$$(+) \qquad \forall z \left[\|z - \varphi(x)^{''}\| < \varepsilon \rightarrow \neg\sigma(z) \right].$$

Verwenden wir nochmals das Transferprinzip 2.23 (für R ersetzt durch R_1, beachte $\varepsilon \in R_1$!), so erhalten wir, dass $(+)$ sogar in $R^{'}$ gilt.

Da nach Voraussetzung $\sigma(x^{'})$ in $R^{'}$ gilt, folgt aus $(+)$ dann:

$$\|x^{'} - \varphi(x^{''})\|^2 \geq \varepsilon^2.$$

Wendet man hierauf den ordnungstreuen Homomorphismus ϱ_1 an, so folgt

$$\|\varrho_1(x^{'}) - \varrho_1 \circ \varphi(x^{''})\|^2 \geq \varrho_1(\varepsilon)^2.$$

Nun ist jedoch $\varrho_1(x^{'}) = x^{''}$ und $\varrho_1 \circ \varphi = \mathrm{id}$. Also folgt $\varrho_1(\varepsilon) = 0$. Dies ist unmöglich, da $\varrho_1|_{R_1}$ ein Isomorphismus und $\varepsilon \in R_1^{\times}$ sind. □

Es bleiben die beiden Hilfssätze zu zeigen.

Beweis. (Hilfssatz 3.28): Der Kern $\mathfrak{p}$ von ϱ ist konvex: sind $0 \leq^{'} a \leq^{'} b \in \mathfrak{p}$ und $a, b \in A^{'}$, so folgt $0 \leq^{''} \varrho(a) \leq^{''} \varrho(b) = 0$, also $\varrho(a) = 0$.

ϱ lässt sich ordnungstreu auf die Lokalisierung $A^{'}_{\mathfrak{p}}$ durch

$$\varrho\left(\frac{a}{b}\right) := \frac{\varrho(a)}{\varrho(b)} \quad \text{mit} \quad a, b \in A^{'},\ b \notin \mathfrak{p}$$

fortsetzen, denn für $0 <^{'} b, d \in A^{'}$ gilt:

$$\begin{aligned} \tfrac{a}{b} \leq' \tfrac{c}{d} &\Rightarrow abd^2 \leq' cdb^2 \\ &\Rightarrow \varrho(abd^2) \leq'' \varrho(cdb^2) \\ &\Rightarrow \tfrac{\varrho(a)}{\varrho(b)} \leq'' \tfrac{\varrho(c)}{\varrho(d)}. \end{aligned}$$

Der Kern dieser Fortsetzung ist $\mathfrak{p}A'_{\mathfrak{p}}$.

Wir bilden dann die konvexe Hülle

$$\mathcal{O} := \{x \in R' \mid |x| \leq' \frac{a}{b} \quad \text{für ein} \quad \frac{a}{b} \in A'_{\mathfrak{p}}\}$$

von $A'_{\mathfrak{p}}$ in R'. Dies ist ein Ring, und somit nach Aufgabe 2.1 ein Bewertungsring. Das maximale Ideal M von $\mathcal{O}$ besteht aus seinen Nichteinheiten, d.h.

$$M = \{x \in R' \mid |x| <' |\frac{a}{b}| \quad \text{für alle} \quad \frac{a}{b} \in A_{\mathfrak{p}}^{\times}\}.$$

M ist konvex in $\mathcal{O}$ (wieder Aufgabe 2.1). Also induziert $\leq'$ eine Anordnung auf dem Restklassenkörper $R_2 := \mathcal{O}/M$. Da R' reell abgeschlossen ist, gilt (nach Aufgabe 2.4) dies auch für R_2. (Man beachte, dass R_2 nicht notwendig Unterkörper von R'' ist.) Der Restklassenhomomorphismus $\varrho_1(x) := x + M$ ist nun die gesuchte Forsetzung von ϱ. Denn es gilt

$$M \cap A'_{\mathfrak{p}} = \mathfrak{p}A'_{\mathfrak{p}}.$$

Da $\mathfrak{p}A'_{\mathfrak{p}}$ das maximale Ideal von $A'_{\mathfrak{p}}$ ist, bleibt nur noch die Inklusion "$\supseteq$" zu zeigen. Seien $a, b >' 0$ mit $\frac{a}{b} \in \mathfrak{p}A'_{\mathfrak{p}}$ gegeben, d.h. $a \in \mathfrak{p}$ und $b \in A' \setminus \mathfrak{p}$. Falls $\frac{a}{b} \notin M$, so gibt es $\frac{c}{d} \in (A'_{\mathfrak{p}})^{\times}$ mit $\frac{c}{d} \leq' \frac{a}{b}$ und $c, d >' 0$. Es folgt dann

$$0 \leq' cb \leq' ad \in \mathfrak{p}$$

und wegen der Konvexität von $\mathfrak{p}$ auch $cb \in \mathfrak{p}$, ein Widerspruch. □

Beweis. (Hilfssatz 3.29) Da $\operatorname{char} R'' = 0$ ist, muss ϱ_1 auf $\mathbb{Z}$ und damit auf $\mathbb{Q}$ die Identität sein. Insbesondere liegt $\mathbb{Q}$ in $\mathcal{O}$. Mit Zorns Lemma erhalten wir dann einen maximalen Teilkörper F von $R_2 = \mathcal{O}/M$ mit einem Schnitt $\varphi\colon F \to \mathcal{O}$, d.h. $\varrho_1 \circ \varphi = \mathrm{id}\,|_F$. Wie üblich schreiben wir $\varrho_1(x) = \overline{x}$ für den Restklassenhomomorphismus.

Wir zeigen, dass F dann gleich R_2 ist. Dazu nehmen wir an, es gäbe $\overline{x} \in R_2 \setminus F$ und unterscheiden zwei Fälle:

1. Fall: $\overline{x}$ ist transzendent über F.
Dann ist aber auch x transzendent über $\varphi(F)$, denn aus

$$x^m + \varphi(a_{m-1})x^{m-1} + \cdots + \varphi(a_0) = 0$$

würde Anwendung von ϱ_1 sofort

$$\overline{x}^m + a_{m-1}\overline{x}^{m-1} + \cdots + a_0 = 0$$

für $a_o, \ldots, a_{m-1} \in F$ ergeben. Damit lässt sich φ von F auf $F(\overline{x})$ durch

$$(++) \qquad \varphi(a_m\overline{x}^m + \cdots + a_0) := \varphi(a_m)x^m + \cdots + \varphi(a_0)$$

zu einem Schnitt von ϱ_1 auf $F(\overline{x})$ fortsetzen. Dies widerspricht jedoch der Maximalität von F.

2. Fall: $\overline{x}$ ist algebraisch über F.
Sei dann $f(X) = \mathrm{Irr}(\overline{x}, F)$. Finden wir zu $\overline{x}$ ein Element $x' \in \mathcal{O}$, das Nullstelle des Bildpolynoms $\varphi(f)(X)$ ist, so können wir wieder mit $(++)$ eine Fortsetzung des Schnittes φ auf $F(\overline{x})$ definieren. Dies würde dann wieder der Maximalität von F widersprechen.
Ebensogut können wir auch eine andere Nullstelle α von f in R_2 folgendermaßen verwenden: Da f eine Nullstelle in R_2 hat (nämlich $\overline{x}$) und R_2 reell abgeschlossen ist, hat $\varphi(f)$ mit dem Transferprinzip 2.23 in R' eine Nullstelle, etwa $x' \in R'$. Da $\varphi(f)$ normiert ist, ist x' ganz über $\varphi(F)$, liegt also in $\mathcal{O}$ ($\mathcal{O}$ ist ganz abgeschlossen in R'). Dann ist aber $\overline{x'}$ Nullstelle von f und wir können $\alpha = \overline{x'}$ setzen. Damit hätten wir wieder einen Widerspruch gegen die Maximalität von F. □

3.4 Der Positivstellensatz

Sei $T \subseteq A$ ein Präpositivbereich. Dann ist

$$T' := \bigcap_{\substack{T \subseteq P \\ P \text{ Positivbereich}}} P$$

ebenfalls ein Präpositivbereich. Im Körperfall ist $T' = T$ (siehe Satz 1.16). Wir fragen uns nun, wie T und T' im Ringfall zusammenhängen.

Beispiel 3.30. $A = \mathbb{R}[X,Y] \ni f = X^2Y^2(X^2+Y^2-1)+1$.
Es gilt $f(a,b) > 0$ für alle $a,b \in \mathbb{R}$, aber $f \notin \sum A^2 =: T$.
Behauptung: $f \in T'$, also $T \subsetneq T'$.
Beweis: Sei $P \in \operatorname{Sper} A$ mit $f \notin P$, also $-f \in P$. Betrachte wieder

$$\alpha_P \colon A \longrightarrow \overline{A} := A/\operatorname{supp} P.$$

Es gilt $\overline{f} := \alpha_P(f) \leq_{\overline{P}} 0$. Weiter ist

$$\overline{A} = \overline{\mathbb{R}[X,X]} = \mathbb{R}[\overline{X},\overline{Y}]$$

und also $\overline{f} = f(\overline{X},\overline{Y}) \leq_{\overline{P}} 0$.
Sei R der reelle Abschluss von $(\operatorname{Quot}\mathbb{R}[\overline{X},\overline{Y}],\overline{P})$ (wobei wir den auf $\operatorname{Quot}\mathbb{R}[\overline{X},\overline{Y}]$ fortgesetzten Positivbereich wieder mit $\overline{P}$ bezeichnen).
Sei S die folgende über $\mathbb{R}$ semialgebraische Menge:

$$S := \{(x,y) \mid f(x,y) \leq 0\}.$$

Dann ist $S(R) \neq \emptyset$, da $(\overline{X},\overline{Y}) \in S$. Also ist auch $S(\mathbb{R}) \neq \emptyset$ (Korollar 2.17). Dies ist ein Widerspruch zu $f(a,b) > 0$ für alle $a,b \in \mathbb{R}$.
Somit liegt f in allen Positivbereichen, also in T'.

In diesem Beispiel wurde eigentlich gezeigt:

Lemma 3.31. *Ist $f \in \mathbb{R}[X_1,\ldots,X_n]$ strikt positiv auf $\mathbb{R}^n$, so auch auf $\operatorname{Sper}\mathbb{R}[X_1,\ldots,X_n]$, d.h.*

$$\alpha_P(f) > 0 \text{ für alle } P \in \operatorname{Sper}\mathbb{R}[X_1,\ldots,X_n].$$

Die analoge Aussage gilt auch für $\geq$.

Satz 3.32 (Positivstellensatz, abstrakt). *Sei T ein Präpositivbereich von A und $f \in A$ strikt positiv auf $\operatorname{Sper}_T^{\max} A$, d.h. $\alpha_P(f) > 0$ für alle $P \in \operatorname{Sper}_T^{\max}$. Dann gibt es $t_1, t_2 \in T$ mit*

$$t_1 f = 1 + t_2.$$

Beweis. Annahme: Solche t_1, t_2 existieren nicht. Dann gilt

$$-1 \notin T - fT =: T_1.$$

Damit ist aber T_1 ein Präpositivbereich über T, welcher $-f$ enthält. Wähle nun einen maximalen Positivbereich P über T_1. Dann ist $P \in \operatorname{Sper}_T^{\max} A$ und $-f \in P$, Widerspruch. □

Satz 3.33 (Positivstellensatz, konkret). *Sei T ein Präpositivbereich von $A = \mathbb{R}[X_1, \ldots, X_n]$ und $f \in \mathbb{R}[X_1, \ldots, X_n]$ sei strikt positiv auf $\mathbb{R}^n$ (d.h. $f(a) > 0$ für alle $a \in \mathbb{R}^n$). Dann hat f die Gestalt*

$$f = \frac{1 + t_2}{t_1}$$

mit $t_1, t_2 \in T$.

Beweis. Folgt sofort aus Lemma 3.31 und dem abstrakten Positivstellensatz. □

Sei nun wieder A beliebiger kommutativer Ring mit $1 \neq 0$ und seien $g_1, \ldots, g_r, h_1, \ldots, h_s \in A$ gegeben. Setze nun

$$G := g_1^{\mathbb{N}} \cdots g_r^{\mathbb{N}} = \text{Menge aller endlichen Produkte der } g_i, \text{ und}$$

$$T = T(h_1, \ldots, h_s) := \sum_{\nu \in \{0,1\}^s} h_1^{\nu_1} \cdots h_s^{\nu_s} \sum A^2.$$

Weiter sei I ein Ideal in A.
Für $P \in \operatorname{Sper} A$ betrachte wieder

$$\begin{aligned} \alpha_P \colon A &\longrightarrow \overline{A} := A/\operatorname{supp} P \\ f &\mapsto \alpha_P(f) =: f(P) \end{aligned}$$

Satz 3.34 (Allgemeiner Positivstellensatz, abstrakt). *Die folgenden beiden Aussagen sind äquivalent:*

(1) Es gibt <u>kein</u> $P \in \operatorname{Sper} A$ mit

$$f(P) = 0 \text{ für alle } f \in I;$$

$$g_j(P) \neq 0 \text{ für } j = 1, \ldots, r;$$

$$h_l(P) \geq 0 \text{ für } l = 1, \ldots, s.$$

(2) Es gibt $b \in I, c \in G$ und $t \in T$ mit

$$c^2 + t = b.$$

Beweis. "(2) $\Rightarrow$ (1)" : Sei $P \in \operatorname{Sper} A$ mit $f(P) = 0$ für alle $f \in I$ sowie $g_j(P) \neq 0$ und $h_l(P) \geq 0$. Dann gilt für alle $c \in G, t \in T$ und $b \in I$:

$$c(P) \neq 0, \text{ also } c(P)^2 > 0,$$

$$t(P) \geq 0 \text{ und } b(P) = 0.$$

Also folgt

$$(c^2 + t)(P) > 0 = b(P),$$

und damit $c^2 + t \neq b$.
"(1) $\Rightarrow$ (2)" : Wir betrachten die Verkettung von drei Homomorphismen:

$$A \longrightarrow A_1 := A/I \longrightarrow A' := (\overline{G})^{-1}A_1 \longrightarrow A'/(P' \cap -P'),$$

die wir wie folgt definieren.

$$\begin{aligned} A &\longrightarrow A/I \\ a &\mapsto \overline{a} := a + I \end{aligned}$$

sei die kanonische Projektion, und setze $\overline{G} := \{\overline{c} \mid c \in G\}$ sowie $\overline{T} := \{\overline{t} \mid t \in T\}$. $\overline{G}$ multiplikativ abgeschlossen, d.h.

$$\overline{G} \cdot \overline{G} \subseteq \overline{G} \text{ und } 1 \in \overline{G}.$$

Falls $0 \in \overline{G}$, so ist $c \in I$ für ein $c \in G$. Dann folgt die Behauptung aber schon mit $t = 0, b = c^2$.
Sei also $0 \notin G$. Dann ist die Lokalisierung $A' := (\overline{G})^{-1}A_1$ von A_1 nach $\overline{G}$ nicht der Nullring. Wir können nun den folgenden Homomorphismus definieren:

$$\begin{aligned} A_1 &\longrightarrow A' \\ \overline{a} &\mapsto \frac{\overline{a}}{\overline{1}}. \end{aligned}$$

Setze schließlich

$$T' := \left\{ \frac{\overline{t}}{\overline{c}^2} \;\middle|\; \overline{t} \in \overline{T}, \overline{c} \in \overline{G} \right\}.$$

T' ist ein Semiring, d.h.

$$T' + T' \subseteq T', \quad T' \cdot T' \subseteq T', \quad (A')^2 \subseteq T'.$$

Es gibt nun zwei Fälle.
1. Fall: $-1 \in T'$. Dann ist also $-1 = \frac{\bar{t}}{\bar{c}^2}$ für ein $t \in T, c \in G$, d.h.

$$\bar{c}_1(\bar{c}^2 + \bar{t}) = 0 \text{ für ein } \overline{c_1} \in \overline{G}.$$

Also gibt es ein $b \in I$ mit

$$(\underbrace{c_1 c}_{\in G})^2 + \underbrace{c_1^2 t}_{\in T} = \underbrace{b}_{\in I}.$$

In diesem Fall ist die Behauptung somit gezeigt.
2. Fall: $-1 \notin T'$. Erweitere T' zu einem $P' \in \operatorname{Sper} A'$ und betrachte die Projektion

$$\alpha_{P'} \colon A' \longrightarrow A'/(P' \cap -P').$$

Sei nun $\alpha \colon A \longrightarrow A'/(P' \cap -P')$ die Verkettung der drei Homomorphismen und setze

$$P := \alpha^{-1}(\alpha_{P'}(P')).$$

Dann ist $P \in \operatorname{Sper} A$ und es gilt

$$b(P') = \alpha(b) = 0 \text{ für alle } b \in I,$$

$$t(P') = \alpha(t) \geq 0 \text{ für alle } t \in T, \text{ da } \frac{\bar{t}}{\bar{1}} \in T' \subseteq P' \text{ und}$$

$$c(P') = \alpha(c) \neq 0 \text{ für alle } c \in G, \text{ da } \bar{c}^2 \text{ und } \frac{1}{\bar{c}^2} \in P'.$$

Dies ist aber ein Widerspruch zur Voraussetzung, also kann dieser Fall gar nicht einteten. □

Satz 3.35 (Allgemeiner Positivstellensatz, konkret). *Sei R reell abgeschlossen und $A = R[X_1, \ldots, X_n]$. Seien $f_1, \ldots, f_m, g_1, \ldots, g_r, h_1, \ldots, h_s \in A$ und G, T wie oben definiert. Sei $I = I(f_1, \ldots, f_m)$ das von den f_i erzeugte Ideal. Dann sind äquivalent:*

(1) $c^2 + t = b$ für gewisse $c \in G, t \in T$ und $b \in I$

(2) für kein $a \in R^n$ gilt gleichzeitig

$$f_i(a) = 0 \text{ für } i = 1, \ldots, m$$
$$g_j(a) \neq 0 \text{ für } j = 1, \ldots, r$$
$$h_l(a) \geq 0 \text{ für } l = 1, \ldots, s.$$

Beweis. Wir zeigen, dass (2) äquivalent dazu ist, dass es kein $P \in \operatorname{Sper} A$ gibt mit

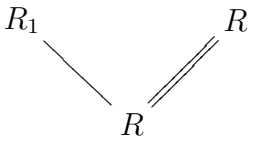
$$\begin{aligned} f_i(P) &= 0 \text{ für } i = 1, \ldots, m \\ g_j(P) &\neq 0 \text{ für } j = 1, \ldots, r \\ h_l(P) &\geq 0 \text{ für } l = 1, \ldots, s. \end{aligned}$$

Dann folgt der Satz sofort aus der abstrakten Version.

Wir nehmen zuerst an, dass es ein solches $P \in \operatorname{Sper} A$ gibt. Wir betrachten wieder

$$\alpha_P \colon A \longrightarrow \overline{A} = R[\overline{X}_1, \ldots, \overline{X}_n]$$

und $\overline{P} := \alpha_P(P)$. Sei R_1 der reelle Abschluss von $(\operatorname{Quot} \overline{A}, \overline{P})$.



Dann gilt für

$$S := \{(x_1, \ldots, x_n) \mid f_i(x) = 0, g_j(x) \neq 0, h_l(x) \geq 0\}$$

offensichtlich $S(R_1) \neq \emptyset$, da $(\overline{X}_1, \ldots, \overline{X}_n) \in S(R_1)$ (denn z.B. $f_i(\overline{X}) = \overline{f_i(X)} = 0$, da $f_i(P) = 0$).

Also ist auch $S(R) \neq \emptyset$, d.h. es gibt ein $a \in R^n$ mit $f_i(a) = 0, g_j(a) \neq 0$ und $h_l(a) \geq 0$. Damit ist die erste Richtung der Äquivalenz gezeigt.

Sei nun umgekehrt $a \in R^n$ mit $f_i(a) = 0, g_j(a) \neq 0$ und $h_l(a) \geq 0$. Betrachte den Einsetzungshomomorphismus

$$\begin{aligned} \varphi_a \colon A &\longrightarrow R \\ f &\mapsto f(a) \end{aligned}$$

und den damit "zurückgezogenen" Positivbereich $P := \varphi_a^{-1}(R^2)$. Für P gilt offensichtlich

$$\begin{aligned} f_i(P) &= 0 \text{ für } i = 1, \ldots, m \\ g_j(P) &\neq 0 \text{ für } j = 1, \ldots, r \\ h_l(P) &\geq 0 \text{ für } l = 1, \ldots, s. \end{aligned}$$

Damit haben wir auch die zweite Richtung der Äquivalenz gezeigt. □

Folgerungen 3.36. Wir ziehen nun einige Folgerungen aus dem Allgemeinen abstrakten Positivstellensatz.

(I)(a) Positivstellensatz, konkret: Sei $f \in R[X_1, \ldots, X_n]$.

Setze $f_1 = 0, g_1 = 1$ und $h_1 = -f$. Wenn f strikt positiv auf $\mathbb{R}^n$ ist, gibt es kein $a \in \mathbb{R}^n$ mit $h_1(a) \geq 0$. Also gibt es nach dem Allgemeinen konkreten Positivstellensatz ein $t \in T$ mit $1 + t = 0$. Wegen $T = \sum A^2 - f \sum A^2$ also $1 + s_1 - fs_2 = 0$ für gewisse $s_i \in \sum A^2$, d.h.

$$fs_2 = 1 + s_1.$$

(I)(b) Seien $f, h_1, \ldots, h_n \in R[X_1, \ldots, X_n]$. Setze $f_1 = 0, g_1 = 1, h_0 = -f$.

Wenn f strikt positiv auf

$$W(h_1, \ldots, h_n) = \{x \in R^n \mid h_1(x) \geq 0, \ldots, h_n(x) \geq 0\}$$

ist, so gibt es kein $a \in R^n$ mit

$$h_0(a) \geq 0, h_1(a) \geq 0, \ldots, h_n(a) \geq 0.$$

Also gibt es nach den Allgemeinen konkreten Positivstellensatz ein $t' \in T' := T(h_0, h_1, \ldots, h_n) = T(h_1, \ldots, h_n) - fT(h_1, \ldots, h_n)$ mit $1 + t' = 0$, also

$$ft_1 = 1 + t_2$$

mit $t_1, t_2 \in T(h_1, \ldots, h_n)$.

(II) Verallgemeinerung des 17. Hilbertschen Problems: Sei f positiv semidefinit auf $W(h_1, \ldots, h_s)$. Setze dann $f_1 = 0, g_1 = f, h_0 = -f$. Dann gilt für alle $a \in R^n$

$$h_i(a) \geq 0 \text{ für } i = 0, \ldots, s \Longrightarrow g_1(a) = 0.$$

Also gilt nach dem Allgemeinen konkreten Positivstellensatz

$$(f^m)^2 + t' = 0$$

für ein $m \in \mathbb{N}$ und $t' \in T' = T(h_1, \ldots, h_s) - fT(h_1, \ldots, h_s)$. Somit erhalten wir die Darstellung

$$ft_2 = f^{2m} + t_1$$

für gewisse $t_1, t_2 \in T(h_1, \ldots, h_s)$. Dies ist eine Verallgemeinerung von Hilberts 17. Problem.

Ausserdem können wir nun in diesem Fall die Frage klären, die wir uns am Anfang dieses Abschnittes gestellt haben. Wir wollten den Zusammenhang zwischen einem Präpositivbereich T und dem Durchschnitt aller darüberliegenden Positivbereiche untersuchen. Falls $f \in P$ für alle $P \in \operatorname{Sper}_{T(h_1,\ldots,h_s)} A$ ist, so erhalten wir wie oben, aber diesmal mit dem Allgemeinen abstrakten Positivstellensatz, die gleiche Darstellung für f. Also gilt

$$\bigcap_{\substack{T(h_1,\ldots,h_s) \subseteq P \\ P \text{ Positivbereich}}} P$$

$$= \left\{ f \mid ft_2 = f^{2m} + t_1 \text{ für gewisse } m \in \mathbb{N}, t_1, t_2 \in T(h_1, \ldots, h_s) \right\}.$$

(III) Reeller Nullstellensatz: Seien $f, f_1, \ldots, f_m \in A = R[X_1, \ldots, X_n]$ mit

$$f = 0 \text{ auf } V(f_1, \ldots, f_m) := \{x \in R^n \mid f_1(x) = 0, \ldots, f_m(x) = 0\}.$$

Dann exisitieren $r \in \mathbb{N}$ und $t \in \sum A^2$ mit

$$f^{2r} + t \in I(f_1, \ldots, f_m).$$

Beweis. Setze $g_1 = f$ sowie $h_1 = 0$, dann gilt nach dem Allgemeinen konkreten Positivstellensatz

$$f^{2r} + t \in I(f_1, \ldots, f_m)$$

für ein $r \in \mathbb{N}$ und ein $t \in T(h_1) = \sum A^2$. □

Definition 3.37. Sei I ein Ideal im kommutativen Ring A. Dann heißt

$$\operatorname{rrad}(I) := \left\{ a \in A \mid a^{2m} + t \in I \text{ für gewisse } m \in \mathbb{N}, t \in \sum A^2 \right\}$$

reelles Radikal von I.
Ein Ideal J heißt *reell*, falls A/J ein reeller Ring ist (vgl. Definition 3.13).

Behauptung 3.38. *Es gilt*

$$\operatorname{rrad}(I) = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ reelles Primideal}}} \mathfrak{p}.$$

Beweis. " $\subseteq$ " : Ist $a \in \operatorname{rrad}(I)$, so also $a^{2m} + t \in I$ für geeignetes $m \in \mathbb{N}, t \in \sum A^2$. Insbesondere gilt natürlich auch für jedes reelle Primideal $\mathfrak{p}$ über I $a^{2m} + t \in \mathfrak{p}$. Also gilt in $A/\mathfrak{p}$

$$\overline{a^{2m} + t} = 0,$$

und da $A/\mathfrak{p}$ reell ist, folgt $\overline{a} = 0$ und somit $a \in \mathfrak{p}$.
" $\supseteq$ " : Sei a aus dem Schnitt über alle reellen Primideale über I. Sei weiter $P \in \operatorname{Sper} A$ mit $I \subseteq \operatorname{supp} P$. Dann ist aber $\operatorname{supp} P$ ein reelles Primideal über I, und somit gilt $a \in \operatorname{supp} P$.
Also gibt es keinen Positivbereich P auf A mit

$$f(P) = 0 \text{ für alle } f \in I \text{ und}$$

$$a(P) \neq 0.$$

Nach dem Allgemeinen abstrakten Positivstellensatz gibt es nun eine Darstellung

$$a^{2m} + t \in I$$

mit gewissem $m \in \mathbb{N}$ und $t \in \sum A^2$. Also ist $a \in \operatorname{rrad}(I)$. □

Bemerkung 3.39. Das *Radikal* eines Ideals I ist definiert als

$$\operatorname{rad}(I) = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ Primideal}}} \mathfrak{p} \quad = \{a \in A \mid a^m \in I \text{ für ein } m \in \mathbb{N}\}.$$

Es gilt der folgende Satz:

Satz 3.40 (Hilbertscher Nullstellensatz). *Sei C ein algebraisch abgeschlossener Körper und $A := C[X_1, \ldots, X_n]$. Sei $I = (f_1, \ldots, f_m)_A$ ein endlich erzeugtes Ideal und sei $f \in A$.*
Gilt dann

$$f(a) = 0 \textit{ für alle } a \in C^n \textit{ mit } f_1(a) = \cdots = f_m(a) = 0,$$

so gilt

$$f \in \operatorname{rad}(I).$$

3.5 Archimedische Ringe

Sei A ein kommutativer Ring mit $1 \neq 0$ und $T \subseteq A$ eine Präordnung.

Definition 3.41. T heißt *archimedisch in* A, falls es zu jedem $a \in A$ ein $n \in \mathbb{N}$ mit $n - a \in T$ gibt.

Bemerkung 3.42. Offensichtlich gilt

$$T \subseteq T',\ T \text{ archimedisch } \implies T' \text{ archimedisch},$$

also insbesondere auch

$$T \subseteq P,\ T \text{ archimedisch und } P \text{ Positivbereich } \implies P \text{ archimedisch }.$$

Wir erinnern uns nun daran, dass wir für einen gegebenen Positivbereich T den Schnitt über alle darüberliegenden Positivbereiche mit T' bezeichnet hatten:

$$T \subseteq T' := \bigcap_{\substack{T \subseteq P \\ P \text{ Positivbereich}}} P.$$

Für die folgende Behauptung benötigen wir auch die Quasi-Kompaktheit von

$$\operatorname{Sper}_T A = \{P \in \operatorname{Sper} A \mid T \subseteq P\}$$

aus Behauptung 3.19 wieder.

Behauptung 3.43. *Wenn alle $P \in \operatorname{Sper}_T A$ archimedisch sind, so auch T'.*

Beweis. Sei $a \in A$ beliebig gegeben. Zu jedem $P \in \operatorname{Sper}_T A$ gibt es nach Voraussetzung ein $n_P \in \mathbb{N}$ mit $n_P - a \in P$.
Sei nun o.B.d.A. immer schon

$$n_p - a \in P^+ := P \setminus -P,$$

was durch Addition von 1 zu n_P immer erreicht werden kann.
Damit haben wir aber eine offene Überdeckung von $\operatorname{Sper}_T A$ in der spektralen Topologie durch die Mengen $U(n_P - a)$ mit $P \in \operatorname{Sper}_T A$. Also folgt aus der Quasi-Kompaktheit schon

$$U(n_{P_1} - a) \cup \ldots \cup U(n_{P_m} - a) \supseteq \operatorname{Sper}_T A$$

für gewisse $P_1, \ldots, P_m \in \operatorname{Sper}_T A$.
Mit $N := \max\{n_{P_1}, \ldots, n_{P_m}\}$ gilt also

$$U(N - a) \supseteq \operatorname{Sper}_T A,$$

und somit $N - a \in P$ für alle $P \in \operatorname{Sper}_T A$, d.h.

$$N - a \in T'.$$

□

Wir können die Aussage des vorigen Beweises auch anders formulieren. Wir haben ja gezeigt, dass

$$N - a > 0 \text{ auf } \operatorname{Sper}_T A$$

für ein passendes $N \in \mathbb{N}$ gilt. Damit erhalten wir aber mit dem Positivstellensatz eine Darstellung

$$t_1(N - a) = 1 + t_2$$

für gewisse $t_1, t_2 \in T$.
Wir geben nun einige Beispiele für archimedische Präpositivbereiche und Positivbereiche.

Beispiele 3.44. (1) $\sum \mathbb{R}^2 = \mathbb{R}^2$ ist archimedisch in $\mathbb{R}$. Ebenso $\sum \mathbb{Q}^2$ in $\mathbb{Q}$.

(2) $A = \mathbb{R}[X]$: Die Positivbereiche P_a, P_{a+}, P_{a-} mit $a \in \mathbb{R}$ (vergleiche Beispiele 3.10(3)) sind alle archimedisch in A. Die Positivbereiche $P_\infty, P_{-\infty}$ sind aber offensichtlich nicht archimedisch, denn die Unbestimmte X bzw. $-X$ ist ja größer als alle reellen Zahlen.

(3) $A = \mathbb{R}(X)$: Hier ist keiner der Positivbereiche archimedisch. Denn egal welche Position die Unbestimmte X bezüglich der reellen Zahlen hat, kann man sich immer ein Element konstruieren, welches größer als alle reellen Zahlen ist. Ist zum Beispiel X infinitesimal kleiner als die Null, so ist $-\frac{1}{X}$ ein solches Element.

(4) Sei X ein kompakter Hausdorffraum, und sei $A = C(X, \mathbb{R})$ der Ring der stetigen Funktionen von X nach $\mathbb{R}$. Dann ist $T := C(X, \mathbb{R}^2)$, die Menge der Funktionen, die nur nichtnegative Werte annehmen, eine archimedische Präordnung auf A. Die Präordnungseigenschaften rechnet

man sofort nach. Da eine stetige Funktion f von X nach $\mathbb{R}$ wegen der Kompaktheit von X immer ihr Maximum annimmt, nimmt die Funktion $N - f$ für ein geeignetes $N \in \mathbb{N}$ nur nichtnegative Werte auf X an (N muss nur größer als das Maximum von f auf X sein). Also ist T archimedisch.

Sei nun A endlich erzeugt über $\mathbb{R}$, d.h. A habe die Gestalt

$$A = \mathbb{R}[x_1, \ldots, x_n].$$

Dann ist

$$I := \{p \in \mathbb{R}[X_1, \ldots, X_n] \mid p(x_1, \ldots, x_n) = 0\}$$

ein Ideal im Polynomring $\mathbb{R}[X_1, \ldots, X_n]$, also

$$I = (p_1, \ldots, p_m)_{\mathbb{R}[X_1, \ldots, X_n]}$$

für gewisse $p_i \in \mathbb{R}[X_1, \ldots, X_n]$. Es gilt

$$A = \mathbb{R}[x_1, \ldots, x_n] = \mathbb{R}[X_1, \ldots, X_n]/I,$$

was man sofort aus dem Homomorphiesatz und der Tatsache, dass die Abbildung

$$\begin{aligned} \mathbb{R}[X_1, \ldots, X_n] &\twoheadrightarrow \mathbb{R}[x_1, \ldots, x_n] \\ p &\mapsto p(x_1, \ldots, x_n) \end{aligned}$$

gerade I als Kern hat, erhält.

Lemma 3.45. *Sei $A = \mathbb{R}[x_1, \ldots, x_n]$, und sei T ein Präpositivbereich von A. Dann sind äquivalent:*

(1) T ist archimedisch

(2) es gibt $N \in \mathbb{N}$ mit $N \pm x_1, \ldots, N \pm x_n \in T$

(3) es gibt $N \in \mathbb{N}$ mit $N - \sum_{i=1}^{n} x_i^2 \in T$

Beweis. (1) $\Rightarrow$ (3): klar.
(3) $\Rightarrow$ (2):

$$\left(N + \frac{1}{4}\right) \pm x_i = \left(\frac{1}{2} \pm x_i\right)^2 + \left(N - \sum_j x_i^2\right) + \sum_{j \neq i} x_j^2 \in T.$$

(2) $\Rightarrow$ (1): Wir zeigen die Aussage: "Zu jedem $f \in \mathbb{R}[X_1, \ldots, X_n]$ gibt es ein $m \in \mathbb{N}$ mit $m - f(x_1, \ldots, x_n) \in T$" durch Induktion über den Aufbau von f.
Falls $f \in \mathbb{R} \cup \{\pm X_1, \ldots, \pm X_n\}$, so ist die Aussage klar. Jedes Element aus $\mathbb{R}$ läßt sich durch ein solches m überschreiten, da T auf $\mathbb{R}$ eingeschränkt ja gerade $\mathbb{R}^2$ ergibt und somit archimedisch in $\mathbb{R}$ ist. Jedes der $\pm X_i$ lässt sich nach (2) überschreiten.
Wir nehmen nun an, dass es für gewisse $f_1, f_2 \in \mathbb{R}[X_1, \ldots, X_n]$ solche $n_1, n_2 \in \mathbb{N}$ gibt mit $n_i \pm f_i(x_1, \ldots, x_n) \in T$ und zeigen die gleiche Aussage für $f_1 + f_2$ sowie für $f_1 \cdot f_2$.
Addition: Es gilt offensichtlich

$$(n_1+n_2)\pm(f_1+f_2)(x_1, \ldots, x_n) = (n_1 \pm f_1(x_1, \ldots, x_n)) + (n_2 \pm f_2(x_1, \ldots, x_n)) \in T.$$

Multiplikation: Es gilt

$$3n_1n_2 - f_1f_2 = (n_1 + f_1)(n_2 - f_2) + n_1(n_2 + f_2) + n_2(n_1 - f_1) \text{ und}$$
$$3n_1n_2 + f_1f_2 = (n_1 + f_1)(n_2 + f_2) + n_1(n_2 - f_2) + n_2(n_1 - f_1).$$

Also folgt

$$3n_1n_2 \pm (f_1f_2)(x_1, \ldots, x_n) \in T.$$

□

Korollar 3.46. *Seien wieder $A = \mathbb{R}[x_1, \ldots, x_n]$ und T ein Präpositivbereich von A. Dann ist*

$$T + \left(N - \sum x_i^2\right) T$$

archimedisch (falls es überhaupt eine Präordnung ist).

Satz 3.47. *Seien $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$, und sei $T = T(h_1, \ldots, h_s)$. Dann gelten*

(1) $-1 \notin T \iff W(h_1, \ldots, h_s) \neq \emptyset$.

(2) T archimedisch $\iff W(h_1, \ldots, h_s)$ kompakt.

Beweis. (1)" $\Leftarrow$ ": Ist $-1 \in T$, so kann $W = W(h_1, \ldots, h_s)$ keine Elemente enthalten, da Elemente aus T offensichtlich immer nichtnegativ auf W sind.
" $\Rightarrow$ ": T ist ein Präpositivbereich. Wähle nun ein $P \in \operatorname{Sper}_T A$. Betrachte die Projektion

$$\alpha_P \colon A \longrightarrow \overline{A} = \mathbb{R}[\overline{x_1}, \ldots, \overline{x_n}]$$

und bezeichne das Bild von P unter α_P mit $\overline{P}$. Sei R der reelle Abschluss von $(\mathrm{Quot}(\overline{A}), \overline{P})$. Wir betrachten die über R semialgebraische Menge

$$S = \{(x_1, \ldots, x_n) \mid h_1(x) \geq 0, \ldots, h_2(x) \geq 0\}.$$

Es gilt $S(R) \neq \emptyset$, da ja $h_i(\overline{x_1}, \ldots, \overline{x_n}) = \overline{h_i} \in \overline{P}$. Wegen $\mathbb{R} \subseteq R$ ist also auch $S(\mathbb{R}) \neq \emptyset$, was aber gerade $W(h_1, \ldots, h_s) \neq \emptyset$ bedeutet.

(2)“ $\Rightarrow$ ”: Sei $N - \sum X_i^2 \in T(h_1, \ldots, h_s)$ für ein geeignetes $N \in \mathbb{N}$. Dann gilt für alle $a \in W(h_1, \ldots, h_s)$ aber $(N - \sum X_i^2)(a) \geq 0$, d.h. also

$$N \geq \sum a_i^2.$$

Also ist W in einer Kugel mit Radius $\sqrt{N}$ enthalten und somit auch kompakt.

“ $\Leftarrow$ ”: Wähle $N \in \mathbb{N}$ so, dass W echt in der Kugel um den Ursprung mit Radius $\sqrt{N}$ liegt. Dann ist nämlich $f := N - \sum X_i^2 > 0$ auf $W(h_1, \ldots, h_s)$. Mit dem konkreten Positivstellensatz erhalten wir $t_1, t \in T(h_1, \ldots, h_s)$ mit $t_1 f = 1 + t$ und also

$$(1 + t)f = t_1 f^2 \in T.$$

Setze $T_0 := \sum A^2 + f \sum A^2$. T_0 ist eine Präordnung, da zum Beispiel $g(0) \geq 0$ für alle $g \in T_0$ gilt. Also kann -1 nicht in T_0 sein. Die anderen Bedingungen sind klar.

Außerdem ist T_0 archimedisch (siehe Korollar 3.46). Es gibt also ein $N' \in \mathbb{N}$ mit $N' - t \in T_0$.

Beachte weiter, dass $(1+t)T_0 \subseteq T$ gilt (denn $(1+t) \in T$ und $(1+t)f \in T$). Somit haben wir

$$f + tN = f + tf + t \sum X_i^2 \in T$$

und

$$(1 + N')(N' - t) = (1 + t)(N' - t) + (N' - t)^2 \in T.$$

Also ist $N' - t \in T$, und damit

$$N(N' + 1) - \sum X_i^2 = NN' + f = (f + tN) + N(N' - t) \in T,$$

. Somit ist T archimedisch. □

Sei nun A wieder ein beliebiger kommutativer Ring und $T \subseteq A$ ein archimedischer Präpositivbereich. Betrachte für $P \in \mathrm{Sper}_T A$ wieder die Projektion

$$\begin{aligned} \alpha_P \colon A &\longrightarrow \overline{A} = A/\operatorname{supp} P \ \supseteq \overline{P}, \ \operatorname{supp} \overline{P} = \{0\} \\ a &\mapsto \overline{a} = \alpha_p(a) = a(P). \end{aligned}$$

Behauptung 3.48. *$\overline{P}$ ist archimedisch in $\overline{A}$.*

Beweis. Für $a \in A$ ist $n - a \in T \subseteq P$ für ein geeignetes $n \in \mathbb{N}$. Also ist

$$\overline{n - a} = n - \overline{a} \in \overline{P}, \text{ d.h. } n \geq_{\overline{P}} \overline{a}.$$

□

Achtung: Quot($\overline{A}$) muss nicht archimedisch bezüglich der fortgesetzen Anordnung $\overline{P}$ sein. Denn $\mathbb{R}[X]$ ist beispielsweise archimedisch bezüglich P_{a+}, aber auf $\mathbb{R}(X)$ gibt es überhaupt keine archimedische Anordnung!

Lemma 3.49. *Sei $T \subseteq A$ archimedisch. Dann gilt für $P \in \operatorname{Sper}_T A$:*

$$\begin{aligned} P \text{ maximal} &\iff \operatorname{Quot}(\overline{A}) \text{ archimedisch bezüglich } \overline{P} \\ &\iff \alpha_P \colon A \longrightarrow \mathbb{R}. \end{aligned}$$

Beweis. Sei P maximal. Wir betrachten wie oben die Projektion α_P und den Positivbereich $\overline{P}$ auf $\overline{A}$, den wir anschließend wieder auf $K = \operatorname{Quot}(\overline{A})$ fortsetzen durch $\frac{\overline{a}}{\overline{b}} \geq 0 \Leftrightarrow \overline{a}\overline{b} \in \overline{P}$. Wir betrachten dann

$$\mathcal{O} := \mathcal{O}(\leq) := \{x \in K \mid |x| \leq m \text{ für ein } m \in \mathbb{N}\}.$$

$\mathcal{O}$ ist ein Bewertungsring von K (vergleiche Aufgabe 2.1) mit maximalem Ideal

$$\mathfrak{m} = \left\{ x \in K \mid |x| < \frac{1}{m} \text{ für alle } m \in \mathbb{N} \right\}.$$

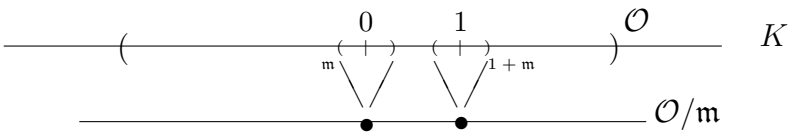
Wir nennen $\mathcal{O}/\mathfrak{m}$ den Restklassenkörper von $\mathcal{O}$ und betrachten den kanonischen Homomorphismus

$$\overline{A} \subseteq \mathcal{O} \xrightarrow{\beta} \mathcal{O}/\mathfrak{m}.$$

$$\begin{array}{ccc} K = \operatorname{Quot}(\overline{A}) & & \\ | & & \\ \mathcal{O} & \xrightarrow{\beta} & \mathcal{O}/\mathfrak{m} \\ | & & \\ A \xrightarrow{\alpha_p} \overline{A} & & \end{array}$$

$\mathcal{O}/\mathfrak{m}$ läßt sich anordnen durch

$$x + \mathfrak{m} \leq y + \mathfrak{m} :\iff x - y \in \mathfrak{m} \vee x \leq_{\overline{P}} y.$$



$(\mathcal{O}/\mathfrak{m}, \leq)$ ist archimedischer Körper, er läßt sich also ordnungstreu in $\mathbb{R}$ einbetten (nach Satz von Hölder, 1.6). Wir haben also insgesamt

$$A \xrightarrow{\alpha_p} \overline{A} \subseteq \mathcal{O} \xrightarrow{\beta} \mathcal{O}/\mathfrak{m} \xhookrightarrow{\gamma} \mathbb{R}$$

und bezeichnen diese Hintereinanderausführung mit δ.

Sei $P' := \delta^{-1}(\mathbb{R}^2) \supseteq P$. Da P' ein Positivbereich ist, folgt aus der Maximalität von P schon $P = P'$. Also ist β eingeschränkt auf $\overline{A}$ schon injektiv. Sonst könnte man nämlich ein Element $\overline{a}$ aus $\overline{A}$ wählen mit $\beta(\overline{a}) = 0$ und $\overline{a} <_{\overline{P}} 0$. Dann wäre aber $a \in P' \setminus P$, Widerspruch.

Also bildet schon α_P nach $\mathbb{R}$ ab, somit ist $\mathrm{Quot}(\overline{A})$ archimedisch angeordnet bezüglich $\overline{P}$.

Sei umgekehrt angenommen

$$\alpha_P \colon A \longrightarrow \mathbb{R} \text{ mit } \overline{P} \subseteq \mathbb{R}^2.$$

Wir wollen zeigen, dass P maximal ist. Sei dazu $P' \supseteq P$. Dann ist $\alpha_P(P') = \overline{P'} \supseteq \overline{P}$ und $\mathfrak{p} := \overline{P'} \cap -\overline{P'}$ ist ein Primideal von $\overline{A}$.

Angenommen es gibt $0 <_{\overline{P}} \overline{a} \in \mathfrak{p}$. Dann gibt es aber auch ein $n \in \mathbb{N}$ mit $1 \leq_{\overline{P}} n\overline{a} \in \mathfrak{p}$, denn wir befinden uns ja nach Voraussetzung in $\mathbb{R}$. Dann ist aber

$$-1 = (\underbrace{n\overline{a} - 1}_{\in \overline{P}}) - \underbrace{n\overline{a}}_{\in \mathfrak{p}} \in \overline{P'},$$

Widerspruch. Also ist $\mathfrak{p} = \{0\} = \operatorname{supp} \overline{P}$ und mit Behauptung 3.6 (2) folgt $\overline{P} = \overline{P'}$, also auch $P = P'$. □

Wieder sei A ein kommutativer Ring und T ein archimedischer Präpositivbereich auf A. Wir bezeichnen nun mit X das maximale Spektrum über T, d.h.

$$X = \operatorname{Sper}_T^{\max} A.$$

Jedes Element $a \in A$ kann man nun als Abbildung auf X auffassen, nämlich durch

$$\begin{aligned} \widehat{a}\colon X &\longrightarrow \mathbb{R} \\ P &\mapsto a(P) = \alpha_P(a). \end{aligned}$$

Nach dem obigen Lemma landen wir so natürlich in $\mathbb{R}$.
Wir versehen nun wieder X mit der spektralen Topologie.

Behauptung 3.50. *Für jedes $a \in A$ ist $\widehat{a} \in C(X, \mathbb{R})$.*

Beweis. Es genügt zu zeigen, dass $\widehat{a}^{-1}((x,\infty))$ und $\widehat{a}^{-1}((-\infty,x))$ für jedes $x \in \mathbb{R}$ offen in der spektralen Topologie auf X ist (denn die Mengen $(x,\infty), (-\infty,x)$ erzeugen gerade die übliche Topologie auf $\mathbb{R}$).
Es gilt

$$\begin{aligned} \widehat{a}^{-1}((x,\infty)) &= \{P \in X \mid x < a(P)\} \\ &= \bigcup_{\substack{x < \frac{r}{s} \\ s,r \in \mathbb{Z} \\ s>0}} \left\{P \in X \mid \frac{r}{s} < a(P)\right\} \\ &= \bigcup_{\substack{x < \frac{r}{s} \\ s,r \in \mathbb{Z} \\ s>0}} \{P \in X \mid r < sa(P)\}. \end{aligned}$$

Es ist aber $\{P \in X \mid r < sa(P)\} = U(sa - r) \cap X$ offen in der spektralen Topologie auf X. Für $(-\infty, x)$ schließen wir analog. □

Wir haben also die Abbildung

$$\begin{aligned} \Phi\colon A &\longrightarrow C(X, \mathbb{R}) \\ a &\mapsto \widehat{a} \end{aligned}$$

mit den folgenden Eigenschaften:

$$\widehat{a+b}(P) = \alpha_P(a+b) = \alpha_P(a) + \alpha_P(b) = \widehat{a}(P) + \widehat{b}(P) \text{ und}$$

$$\widehat{a \cdot b}(P) = \alpha_P(a \cdot b) = \alpha_P(a) \cdot \alpha_P(b) = \widehat{a}(P) \cdot \widehat{b}(P)$$

für alle $P \in X$. Also gilt $\widehat{a+b} = \widehat{a} + \widehat{b}$ und $\widehat{a \cdot b} = \widehat{a} \cdot \widehat{b}$. Ebenso gilt $\widehat{1} = 1$, denn $\widehat{1}(P) = \alpha_P(1) = 1$ für alle $P \in X$. Somit ist Φ ein Ringhomomorphismus.

Satz 3.51 (Darstellungssatz). *Sei A ein kommutativer Ring mit $\mathbb{Q} \subseteq A$ und sei $T \subseteq A$ ein archimedischer Präpositivbereich. Dann definiert $a \mapsto \widehat{a}$ einen Ringhomomorphismus*

$$\Phi_T \colon A \longrightarrow C(X, \mathbb{R}),$$

wobei $X := \operatorname{Sper}_T^{\max} A$ mit der spektralen Topologie versehen ist. Es gelten

(1) $\widehat{a} > 0$ auf $X \Longrightarrow a \in T$.

(2) $\widehat{a} \geq 0$ auf $X \Longleftrightarrow a + r \in T$ für alle $r \in \mathbb{Q}$ mit $0 < r$.

(3) $\widehat{a} = 0$ auf X (also $a \in \operatorname{Kern} \Phi_T$) $\Longleftrightarrow r \pm a \in T$ für alle $r \in \mathbb{Q}$ mit $0 < r$.

(4) $\Phi_T(A)$ ist dicht in $C(X, \mathbb{R})$ bezüglich der Maximumsnorm, d.h. zu jedem $f \in C(X, \mathbb{R})$ und jedem $\varepsilon > 0$ gibt es ein $a \in A$ mit $\|\widehat{a} - f\|_\infty < \varepsilon$.

Beweis. (4): Folgt aus dem Satz von Stone-Weierstraß (vgl. Aufgabe 10.2): $C(X, \mathbb{R})$ ist bezüglich der Maximumsnorm eine vollständige $\mathbb{R}-$Algebra und $\Phi_T(A)$ ist eine $\mathbb{Q}-$Unteralgebra davon. $\Phi_T(A)$ liegt dicht in $C(X, \mathbb{R})$, falls $\Phi_T(A)$ "Punkte" trennt, d.h. falls es zu $P_1, P_2 \in X$ mit $P_1 \neq P_2$ ein $\widehat{a} \in \Phi_T(A)$ gibt mit $\widehat{a}(P_1) \neq \widehat{a}(P_2)$. Dies ist aber in diesem Fall erfüllt, denn man wähle einfach ein $a \in P_1 \setminus P_2$. Dann erhält man

$$\widehat{a}(P_1) = \alpha_{P_1}(a) \geq 0 > \alpha_{P_2}(a) = \widehat{a}(P_2).$$

(3): Folgt aus (2).
(2): Folgt aus (1), denn " $\Rightarrow$ " ist offensichtlich mit (1) und " $\Leftarrow$ " erhält man so:

$$a + r \in T \Longrightarrow 0 \leq \alpha_P(a + r) = \alpha_P(a) + r$$

für alle $P \in X$. Gilt dies für alle $r \in \mathbb{Q}$ mit $r > 0$, so folgt schon $\alpha_P(a) \geq 0$ für alle $P \in X$.
(1): Sei $\widehat{a}(P) = \alpha_P(a) > 0$ für alle $P \in X = \operatorname{Sper}_T^{\max} A$. Dann erhalten wir mit dem abstrakten Positivstellensatz (3.32) gewisse $t, t_1 \in T$ mit $ta = 1 + t_1$.
Da T archimedisch ist, gibt es $m, l \in \mathbb{N}$ mit $l - t, m + a \in T$. Wir zeigen nun, dass für alle $r \in \mathbb{N}$ gilt:

$$a + \frac{r}{l} \in T \Longrightarrow a + \left(\frac{r}{l} - \frac{1}{l}\right) \in T.$$

Denn:

$$l^2a + (rl - l) = \underbrace{(l-t)}_{\in T}\underbrace{(la+r)}_{\in T} + l\underbrace{(ta-1)}_{\in T} + tr \in T.$$

Multiplizieren wir nun mit $\frac{1}{l^2}$ (es gilt $\mathbb{Q} \subseteq A$ und daher $\mathbb{Q}^+ \subseteq T$), so erhalten wir das Resultat.

Wir beginnen nun also mit der Tatsache, dass $a + \frac{ml}{l} \in T$ gilt, und iterieren das obige Resultat, bis wir schließlich

$$\left(a + \frac{ml}{l}\right) - \frac{ml}{l} = a \in T$$

erhalten. □

Satz 3.52 (Schmüdgen). *Seien $f, h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n] =: A$. Sei weiter*

$$W(h_1, \ldots, h_s) = \{x \in \mathbb{R}^n \mid h_1(x) \geq 0, \ldots, h_s(x) \geq 0\}$$

kompakt. Falls dann

$$f > 0 \text{ auf } W(h_1, \ldots, h_s)$$

gilt, so folgt

$$f \in T(h_1, \ldots, h_s).$$

Beweis. Da $W = W(h_1, \ldots, h_s)$ kompakt ist, ist $T = T(h_1, \ldots, h_s)$ archimedisch nach Satz 3.47.

Sei $P \in \operatorname{Sper}_T^{\max} A$. Dann gilt nach Lemma 3.49: $\alpha_P \colon A \longrightarrow \mathbb{R}$, d.h. für alle $g \in \mathbb{R}[X_1, \ldots, X_n]$ ist

$$\alpha_P(g) = g(\underbrace{\alpha_P(X_1), \ldots, \alpha_P(X_n)}_{\in \mathbb{R}^n}) = g(\underbrace{\overline{X_1}, \ldots, \overline{X_n}}_{\in \mathbb{R}^n}).$$

Da $T \subseteq P$, folgt

$$0 \leq \alpha_P(h_i) = h_i(\overline{X_1}, \ldots, \overline{X_n}) \text{ für } i = 1, \ldots, s,$$

somit ist

$$(\overline{X_1}, \ldots, \overline{X_n}) \in W.$$

Also gilt nach Voraussetzung

$$0 < f(\overline{X_1}, \ldots, \overline{X_n}) = \alpha_P(f),$$

d.h. $\widehat{f}$ (definiert wie im Darstellungssatz) ist strikt positiv auf $\mathrm{Sper}_T^{\max} A$. Dann liefert der Darstellungssatz aber

$$f \in T(h_1, \ldots, h_s).$$

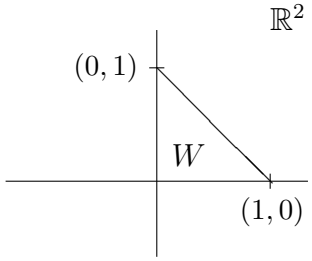
□

Wir schauen uns nun Beispiele zum Satz von Schmüdgen an.

Beispiele 3.53. - Wir wählen $n = 2$ und

$$h_1 = X_1,\ h_2 = X_2,\ h_3 = 1 - (X_1 + X_2)\,.$$

Dann ist die Menge $W = W(h_1, h_2, h_2)$ das folgende (kompakte) Dreieck im ersten Quadranten des $\mathbb{R}^2$:



Nach dem Satz von Schmüdgen hat also jedes reelle Polynom f in zwei Unbestimmten, welches strikt positiv auf dieser Menge W ist, eine Darstellung der folgenden Gestalt:

$$\begin{aligned} f = \sigma_0 &+ \sigma_1 X_1 + \sigma_2 X_2 + \sigma_3 (1 - X_1 - X_2) \\ &+ \sigma_4 X_1 X_2 + \sigma_5 X_1 (1 - X_1 - X_2) \\ &+ \sigma_6 X_2 (1 - X_1 - X_2) + \sigma_7 X_1 X_2 (1 - X_1 - X_2) \end{aligned}$$

mit gewissen $\sigma_i \in \sum \mathbb{R}[X_1, X_2]^2$.

- Die Bedingung "W kompakt" kann im Satz von Schmüdgen nicht weggelassen werden. Denn etwa:

$$f := X^4Y^2 + X^2Y^4 - 3X^2Y^2 + 2 > 0 \text{ auf } \mathbb{R}^2,$$

aber $f \notin \sum \mathbb{R}[X, Y]^2$ (vgl. Aufgabe 5.3), was man aber aus dem Satz von Schmüdgen ohne die Kompaktheit bekäme mit $s = 1, h_1 = 1$.

- Die Bedingung "$f > 0$" kann im Satz von Schmüdgen nicht abgeschwächt werden zu "$f \geq 0$". Siehe dazu Aufgabe 10.3.

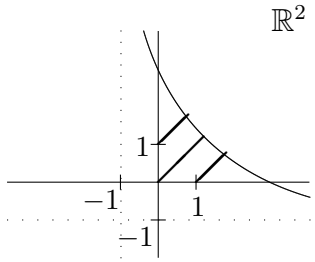
- Die echten Produkte $h_1^{\nu_1} h_2^{\nu_2} \cdots h_s^{\nu_s}$, die in der Darstellung für f im Satz von Schmüdgen auftreten, können im Allgemeinen nicht (alle) weggelassen werden, d.h. für $f > 0$ auf $W(h_1, \ldots, h_s)$ können wir im Allgemeinen nicht

$$f = \sigma_0 + \sigma_1 h_1 + \cdots + \sigma_s h_s$$

mit Quadratsummen σ_i erwarten. Ein Beispiel dafür ist das folgende (wieder mit $n = 2$):

$$h_1 = X_1,\ h_2 = X_2,\ h_3 = 4 - (X_1 + 1)(X_2 + 1)$$

Dann ist $W(h_1, h_2, h_3)$ die folgende kompakte Menge:



Sei nun N so gewählt, dass $f := N - (X_1^2 + X_2^2) > 0$ auf W gilt (z.B. $N = 10$). Es gilt aber

$$f \notin \sum + \sum h_1 + \sum h_2 + \sum h_3 \quad \left(\sum := \sum \mathbb{R}[X_1, X_2]^2\right).$$

Dies sieht man am besten folgendermaßen: Wir definieren uns die Menge $S \subseteq \mathbb{R}[X_1, X_2]$ wie folgt. Wir ordnen für ein gegebenes Polynom $p \in \mathbb{R}[X_1, X_2] \setminus \{0\}$ die Monome lexikographisch nach ihren Hochzahlen und betrachten das größte nichtverschwindende Monom $p_{(n,m)} X_1^n X_2^m$ mit $n, m \in \mathbb{N}_0$ und $p_{(n,m)} \in \mathbb{R}$. Dann berechnen wir n und m modulo 2, d.h. (n, m) ist kongruent zu einer der folgenden vier Möglichkeiten:

$$(0,0),\ (1,0),\ (0,1),\ (1,1).$$

Schließlich definieren wir (für $p \neq 0$): $p \in S$ genau dann wenn entweder

$$(n,m) \equiv (0,0), (1,0), (0,1) \text{ und } p_{(n,m)} \geq 0$$

oder

$$(n,m) \equiv (1,1) \text{ und } p_{(n,m)} \leq 0.$$

Zudem fordern wir $0 \in S$.

Man sieht leicht, dass S abgeschlossen ist bezüglich Addition und unter Multiplikation mit Quadraten, d.h.

$$S + S \subseteq S \text{ und } \mathbb{R}[X_1, X_2]^2 \cdot S \subseteq S.$$

Weiter gilt offensichtlich $h_1, h_2, h_3 \in S$. Damit müsste aber f, wenn es eine Darstellung

$$f = \sigma_0 + \sigma_1 h_1 + \sigma_2 h_2 + \sigma_3 h_3 \quad \left(\sigma_i \in \sum \mathbb{R}[X_1, X_2]^2\right)$$

hätte, auch in S sein, was aber offensichtlich nicht der Fall ist.

4 Quadratische Moduln

In diesem Kapitel wollen wir eine Verschärfung des Satzes 3.52 von Schmüdgen bereitstellen.

4.1 Semi-Ordnungen auf Körpern

Definition 4.1. Sei K ein Körper. Eine Teilmenge M von K heißt *quadratischer Modul* von K, falls gilt:

$$M + M \subseteq M, \quad MK^2 \subseteq M, \quad 1 \in M, \quad -1 \notin M.$$

Gilt zusätzlich noch $M \cup -M = K$, so heißt M eine *Semi-Ordnung* von K.

Jede Präordnung von K ist automatisch ein quadratischer Modul. Es gibt jedoch quadratische Moduln, die nicht unter Multiplikation abgeschlossen sind. In Beispiel 3.53 hatten wir eine Teilmenge S von $\mathbb{R}[X_1, X_2]$ definiert. Erweitert man die dortige Definition auf $\mathbb{R}(X_1, X_2)$ indem man setzt

$$\frac{f}{g} \in S' :\Leftrightarrow fg \in S,$$

wobei $f, g \in \mathbb{R}[X_1, X_2]$ mit $g \neq 0$ sind, so ist S' ein quadratischer Modul von $\mathbb{R}(X_1, X_2)$, jedoch keine Präordnung.

$\sum K^2$ ist der kleinste quadratische Modul von K, falls K reell ist. Besitzt K einen quadratischen Modul, so ist umgekehrt K reell.

Lemma 4.2. *Ist $S \subseteq K$ eine Semi-Ordnung und definiert man $a \leq_S b$, falls $b - a \in S$ ist, so gelten*

1. $a \leq a$,
2. $a \leq b, b \leq c \Rightarrow a \leq c$,
3. $a \leq b, b \leq a \Rightarrow a = b$,
4. $a \leq b$ *oder* $b \leq a$,
5. $a \leq b \Rightarrow a + c \leq b + c$,
6. $a \leq b \Rightarrow ac^2 \leq bc^2$.

(Wir schreiben kurz $\leq$, wenn die Abhängigkeit von S klar ist.)

Beweis. Alle Eigenschaften bis auf 3. sind klar. Für 3. bleibt zu zeigen: $x, -x \in S \Rightarrow x = 0$.

Wäre $x \neq 0$, so hätten wir

$$-1 = x\left(\frac{1-x^{-1}}{2}\right)^2 + (-x)\left(\frac{1+x^{-1}}{2}\right)^2 \in S.$$

Man beachte, dass K reell, also $\operatorname{char} K \neq 2$ ist. □

Bemerkung 4.3. Erfüllt eine zweistellige Relation $x \leq y$ die Eigenschaften 1.-6., so ist umgekehrt

$$S = \{x \in K \mid 0 \leq x\}$$

eine Semi-Ordnung von K.

Lemma 4.4. *Ist $\leq$ eine Semi-Ordnung von K, so gelten weiter*

7. $0 < a \Rightarrow 0 < \frac{1}{a}$,
8. $0 < a < b \Rightarrow ba^2 < ab^2$,
9. $0 < a < b \Rightarrow 0 < \frac{1}{b} < \frac{1}{a}$,
10. $0 < a < m \Rightarrow a^2 < m^2$, *für* $m \in \mathbb{N}$,
11. $m < a \Rightarrow m^2 < a^2$, *für* $m \in \mathbb{N}$.

Beweis. 7. Ist $0 < a$, so gilt $0 < a(\frac{1}{a})^2 = \frac{1}{a}$.
8. Aus $0 < a$ und $0 < b - a$ folgt mit 7.:

$$0 < \frac{1}{\frac{1}{b-a} + \frac{1}{a}} b^2 = ab^2 - ba^2.$$

9. folgt mit 8. aus: $\frac{1}{b} = ba^2(\frac{1}{ab})^2 < ab^2(\frac{1}{ab})^2 = \frac{1}{a}$.
10. Aus $0 < a < m$ folgt mit 8.: $ma^2 < am^2$. Wegen $\frac{1}{m} \in \sum K^2$ folgt daraus $a^2 < am$. Andererseits folgt wegen $m \in \sum K^2$ aus $a < m$ die Ungleichung $am < m^2$. Zusammen ergibt dies $a^2 < m^2$.
11. zeigt man analog zu 10. □

Satz 4.5. *Ist $\leq$ eine archimedische Semi-Ordnung von K (d.h. zu jedem $a \in K$ gibt es ein $n \in \mathbb{N}$ mit $a \leq n$), so ist $\leq$ eine (archimedische) Anordnung von K, also ist K isomorph zu einem Teilkörper von $\mathbb{R}$.*

Beweis. Wir zeigen zuerst, dass $\mathbb{Q}$ dicht in K bzgl. $\leq$ ist:

Sei $0 < c < d$. Dann folgt $0 < (d-c)^{-1} < q$ für ein $q \in \mathbb{N}$. Hieraus folgt mit 9. erst $\frac{1}{q} < d - c$ und dann $1 < q(d-c)$, da $q \in \sum K^2$ ist. Hieraus erhalten wir

$$qc < qd - 1.$$

Sei nun $p \in \mathbb{N}$ minimal mit $qd \leq p + 1$. Dann folgt

$$qc < qd - 1 \leq p < qd.$$

Wegen $\frac{1}{q} \in \sum K^2$ folgt daraus $c < \frac{p}{q} < d$.

Als nächstes zeigen wir, dass mit $0 < a, b$ auch $0 < ab$ ist. Es sei etwa $0 < a < b$. Wir setzen dann $c := b - a$ und $d := b + a$. Also gilt $0 < c < d$. Nach dem oben Gezeigten gibt es $p, q \in \mathbb{N}$ mit

$$qc < p < qd.$$

Mit 10. und 11. folgt dann

$$q^2c^2 < p^2 < q^2d^2.$$

Dies ergibt insbesondere

$$(b-a)^2 = c^2 < d^2 = (b+a)^2,$$

also $0 < 4ab$, und schließlich $0 < ab$. □

Satz 4.6. *Sei S eine Semi-Ordnung von K. Dann ist*

$$\mathcal{O}(S) := \{a \in K \mid |a| \leq_S m \text{ für ein } m \in \mathbb{N}\}$$

ein konvexer Unterring mit einem einzigen maximalen Ideal

$$\mathcal{M}(S) := \{a \in K \mid |a| <_S \frac{1}{m} \text{ für alle } m \in \mathbb{N} \setminus \{0\}\}.$$

Der Restklassenhomomorphismus $a \overset{\varrho}{\mapsto} \overline{a} := a + \mathcal{M}(S)$ bildet $S \cap \mathcal{O}(S)$ auf eine archimedische Semi-Ordnung $\overline{S} := \overline{S \cap \mathcal{O}(S)}$ des Restklassenkörpers $\overline{K} := \mathcal{O}(S)/\mathcal{M}(S)$ ab. Insbesondere ist dann $(\overline{K}, \leq_{\overline{S}})$ ordnungstreu in $\mathbb{R}$ einbettbar.

Beweis. Wir schreiben kurz $\mathcal{O}$ und $\mathcal{M}$ für $\mathcal{O}(S)$ und $\mathcal{M}(S)$.
Die Inklusion $\mathcal{O} \pm \mathcal{O} \subseteq \mathcal{O}$ ist sofort klar. Wir zeigen nun $\mathcal{O}^2 \subseteq \mathcal{O}$. Daraus folgt dann für $a, b \in \mathcal{O}$ auch

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \in \mathcal{O}.$$

Sei also $a \in \mathcal{O}$, etwa $0 < a$. Nach Definition von $\mathcal{O}$ gibt es dann ein $m \in \mathbb{N}$ mit $0 < a \leq m$. Hieraus folgt mit Lemma 4.4, 10. aber $a^2 \leq m^2$. Also ist auch $a^2 \in \mathcal{O}$.
Die Konvexität von $\mathcal{O}$ folgt direkt aus der Definition. Weiter sieht man mit 4.4, 9., dass ein positives $a \in K$ genau dann eine Einheit in $\mathcal{O}$ ist, wenn es positive rationale Zahlen r und s mit

$$r \leq a \leq s$$

gibt. Hieraus erkennt man, dass $\mathcal{M}$ die Menge der Nichteinheiten von $\mathcal{O}$ ist. Da $\mathcal{M}$ offensichtlich ein $\mathcal{O}$-Ideal ist, muss $\mathcal{M}$ ein maximales Ideal sein, das alle anderen Ideale umfasst.
Um einzusehen, dass $\overline{S}$ eine Semi-Ordnung von $\overline{K}$ ist, muss man lediglich $-\overline{1} \notin \overline{S}$ prüfen. Falls jedoch $-\overline{1} = \overline{s}$ für ein $s \in \mathcal{O} \cap S$, so wäre $1 + s \in \mathcal{M}$, was offensichtlich nicht der Fall ist. Die Archimedizität von $\overline{S}$ folgt sofort aus der Definition von $\mathcal{O}$.

Nach Satz 4.5 ist dann $(\overline{K}, \leq_{\overline{S}})$ ein archimedisch angeordneter Körper, also nach dem Satz 1.6 von Hölder in $\mathbb{R}$ ordnungstreu einbettbar. □

Zusatz 4.7. *$\mathcal{O}(S)$ ist ein Bewertungsring von K, d.h. ist $a \notin \mathcal{O}(S)$, so gilt $a^{-1} \in \mathcal{O}(S)$.*

Beweis. Ist $a \notin \mathcal{O}(S)$ und etwa $0 < a$, so gilt $m < a$ für alle $m \in \mathbb{N}$. Dann folgt mit 4.4, 9. aber $0 < a^{-1} < \frac{1}{m}$ für alle $m \in \mathbb{N} \setminus \{0\}$. Also ist $a^{-1} \in \mathcal{M}(S)$. □

4.2 Quadratische Moduln auf Ringen

Definition 4.8. Sei A ein kommutativer Ring mit $1 \neq 0$. Eine Teilmenge M von A heißt *quadratischer Modul* von A, falls

$$M + M \subseteq M, \quad MA^2 \subseteq M, \quad 1 \in M, \quad -1 \notin M.$$

Gilt zusätzlich noch $M \cup -M = A$ und $M \cup -M$ ist ein A-Primideal, so heißt M eine *Semi-Ordnung* von A.

Für $a_1, \ldots, a_s \in A$ schreiben wir

$$M(a_1, \ldots, a_s) := \sum A^2 + a_1 \sum A^2 + \cdots + a_s \sum A^2.$$

Es gilt dann $-1 \notin M(a_1, \ldots, a_s)$ genau dann, wenn $M(a_1, \ldots, a_s)$ ein quadratischer Modul von A ist. Man beachte, dass für $a \in A$ die Menge $M(a)$ sogar multiplikativ abgeschlossen ist, also für $-1 \notin M(a)$ ist $M(a)$ eine Präordnung von A.

Lemma 4.9. *Ist $M \subseteq A$ maximaler quadratischer Modul von A, so gilt zusätzlich:*

$$M \cup -M = A \text{ und } M \cap -M \text{ ist ein } A\text{-Primideal,}$$

d.h. M ist eine Semi-Ordnung von A.

Beweis. Sei $a \notin M \cup -M$. Da M maximal ist, können $M + a\sum A^2$ und $M - a\sum A^2$ dann keine quadratischen Moduln sein. Also gibt es $m_1, m_2 \in M$ und $\sigma_1, \sigma_2 \in \sum A^2$ mit

$$-1 = m_1 + a\sigma_1 \quad \textit{und} \quad -1 = m_2 - a\sigma_2.$$

Wegen

$$0 = \sigma_1(\sigma_2 a) + \sigma_2(-\sigma_1 a) = \sigma_1 + \sigma_1 m_2 + \sigma_2 + \sigma_2 m_1$$

folgt dann

$$-\sigma_1 = \sigma_2 + \sigma_1 m_2 + \sigma_2 m_1 \in M.$$

Weiter folgt

$$\begin{aligned} -4 = 4(m_1 + a\sigma_1) &= 4m_1 + ((a+1)^2 - (a-1)^2)\sigma_1 \\ &= 4m_1 + (a+1)^2\sigma_1 + (a-1)^2(-\sigma_1) \in M, \end{aligned}$$

und schließlich $-1 = -4 + 3 \in M$, ein Widerspruch.

Also ist $M \cup -M = A$. Setzt man $I = M \cap -M$, so sieht man sofort die Inklusionen

$$I + I \subseteq I \quad \text{und} \quad \pm IA^2 \subseteq I$$

ein. Um zu sehen, dass I ein A-Ideal ist, seien $a \in A$ und $b \in I$. Wegen $4a = (a+1)^2 - (a-1)^2$ folgt dann

$$4ab \in IA^2 - IA^2 \subseteq I.$$

Falls $ab \notin I$, so muss $ab \notin M$ oder $-ab \notin M$ gelten. Wegen $M \cup -M = A$ folgt dann

$$-ab \in M \quad \text{oder} \quad ab \in M.$$

Im ersten Fall folgt

$$ab = 4ab - 3ab \in M$$

und im zweiten Fall

$$-ab = -4ab + 3ab \in M.$$

Also wäre doch $ab \in I$, ein Widerspruch.

Es bleibt zu zeigen, dass I ein Primideal von A ist. Seien also $ab \in I$ und $b \notin I$. Falls $b \notin M$, so folgt $-1 \in b\sum A^2 + M$, da M maximal ist. Also erhalten wir

$$-a^2 \in a(ab)\sum A^2 + M \subseteq I + M \subseteq M.$$

Also insgesamt $a^2 \in I$. Für $-b \notin M$ erhält man analog auch $a^2 \in I$.

Falls jetzt $a \notin M$, so ist wieder $-1 \in a\sum A^2 + M$. Sei etwa $-1 = a\sigma + m$ mit $m \in M$ und $\sigma \in \sum A^2$. Dann folgt

$$(1+m)^2 = a^2\sigma^2 \in I.$$

Damit läge $-1 - (2m + m^2)$ in I. Also folgt

$$-1 \in M + I \subseteq M.$$

Dies ist unmöglich, also gilt $a \in M$. Analog erhält man $-a \in M$, insgesamt also $a \in I$. □

Sei jetzt M ein quadratischer Modul von A. Wir setzen dann

$$Y_M := \text{ Semi-Sper}_M A = \{S \subseteq A \mid S \text{ Semi-Ordnung von } A, M \subseteq S\}.$$

Die Menge Y_M umfasst selbstverständlich das reelle Sepektrum von A über M:

$$X_M := \text{ Sper}_M A = \{P \subseteq A \mid P \text{ Positivbereich von } A, M \subseteq P\}.$$

Mit $Y_M^{\max}$ und $X_M^{\max}$ bezeichnen wir die Teilmengen von Y_M bzw. X_M bestehend aus den maximalen Elementen. Wie in Kapitel 3 für Präpositivbereiche nennen wir jetzt einen quadratischen Modul M von A *archimedisch*, falls es zu jedem $a \in A$ ein $n \in \mathbb{N}$ mit $n - a \in M$ gibt.

Unser nächstes Ziel ist es, für archimedische Moduln M die Gleichheit $X_M^{\max} = Y_M^{\max}$ zu zeigen, sowie den Darstellungsatz 3.51 zu verschärfen.

Lemma 4.10. *Ist $M \subseteq A$ ein archimedischer quadratischer Modul von A, so gilt $X_M^{\max} = Y_M^{\max}$.*

Beweis. Sei $S \in Y_M$. Wie bei Positivbereichen definieren wir den kanonischen Homomorphismus

$$\alpha_S : A \to A/(S \cap -S) = \overline{A}.$$

Das Bild $\overline{S}$ von S unter α_S ist wieder eine Semi-Ordnung von $\overline{A}$ mit der Eigenschaft

$$\overline{S} \cap -\overline{S} = \{\overline{0}\}.$$

Eine Semi-Ordnung $\overline{S}$ eines Integritätsbereiches $\overline{A}$ mit $\overline{S} \cap -\overline{S} = \{\overline{0}\}$ lässt sich zu einer Semi-Ordnung S' des Quotientenkörpers $F = \operatorname{Quot} \overline{A}$ (ebenso wie bei Positivbereichen in Behauptung 3.7) durch die Definition

$$\frac{\overline{a}}{\overline{b}} \in S' :\Leftrightarrow \overline{a}\overline{b} \in \overline{S}$$

fortsetzen.

Wir erhalten dann die folgende Komposition von Homomorphismen

$$\alpha : A \xrightarrow{\alpha_S} \overline{A} \subseteq \mathcal{O}(\overline{S}) \xrightarrow{\varrho} \mathcal{O}(\overline{S})/\mathcal{M}(\overline{S}) \xrightarrow{\iota} \mathbb{R}.$$

Dabei ist α_S der kanonische Homomorphismus von oben. Wegen der Archimedizität von M gibt es zu $a \in A$ ein $n \in \mathbb{N}$ mit $n - a \in M \subseteq S$. Also gilt auch $\overline{n} - \overline{a} \in \overline{S}$. Hieraus folgt $\overline{A} \subseteq \mathcal{O}(\overline{S})$. Nach Satz 4.5 ist der Restklassenkörper $\mathcal{O}(\overline{S})/\mathcal{M}(\overline{S})$ archimedisch angeordnet, lässt sich also mit ι ordnungstreu in $\mathbb{R}$ einbetten. Insgesamt gilt also

$$\alpha(S) \subseteq \mathbb{R}^2.$$

Sei weiter $P_S = \alpha^{-1}(\mathbb{R}^2)$. Dies ist ein Positivbereich $P_S \in X_M$ mit $S \subseteq P_S$.

Ist jetzt $S \in Y_M^{\max}$, so folgt sofort $S = P_S$ und damit $S \in X_M^{\max}$.

Ist umgekehrt $P \in X_M^{\max}$ und $S \in Y_M$ mit $P \subseteq S$, so folgt $P \cap -P \subseteq S \cap -S =: \mathfrak{p}$. Der Homomorphismus $\alpha_P : A \to \overline{A} \subseteq \mathbb{R}$ (vgl. den Beweis von Lemma 3.49) sendet $\mathfrak{p}$ auf ein $\overline{A}$-Ideal $\overline{\mathfrak{p}}$ in $\mathbb{R}$. Wie in 3.49 ergibt sich dann $\overline{\mathfrak{p}} = \{\overline{0}\}$, d.h. $P \cap -P = S \cap -S$. Nun folgt sofort $P = S$. □

Darstellungssatz 4.11. *(T. Jacobi) Sei A ein kommutativer Ring mit $\mathbb{Q} \subseteq A$. Ist $M \subseteq A$ ein archimedischer quadratischer Modul, dann gilt $Y_M^{\max} = X_M^{\max}$ und die Zuordnung $a \to \widehat{a}$ (mit $\widehat{a} : X_M^{\max} \to \mathbb{R}$ definiert durch $\widehat{a}(P) = \alpha_P(a)$) definiert einen Homomorphismus*

$$\Phi_M : A \to C(X_M^{\max}, \mathbb{R}),$$

für den gilt:

$$\widehat{a} > 0 \quad \text{auf} \quad X_M^{\max} \quad \Rightarrow \quad a \in M.$$

Des Weiteren gelten analoge Aussagen zu Satz 3.51.

Beweis. Falls $-1 \notin M - a\sum A^2 =: M_1$, so ist M_1 ein quadratischer Modul von A, der M enthält. Ist dann $S \supseteq M_1$ maximal, so gilt $S \in Y_M^{\max}$ und $-a \in S$. Also

$$\widehat{a}(S) = \alpha_S(a) \leq 0.$$

Ist also $\widehat{a} > 0$ auf $X_M^{\max} = Y_M^{\max}$, so gibt es $s \in M$ und $t \in \sum A^2$ mit $-1 = s - at$, also

$$ta - 1 \in M.$$

Da M archimedisch ist, gibt es positive rationale Zahlen r und k mit

$$a + r \in M \quad \text{und} \quad 2k - 1 - t^2 a \in M.$$

Es gilt dann

$$2k - t = (2k - 1 - t^2 a) + t(ta - 1) + 1 \in M.$$

Hieraus folgt

$$k^2 a + k^2 r - 1 = (k-t)^2(a+r) + 2k(ta-1) + rt(2k-t) + (2k-1-t^2 a) \in M.$$

Diese letzte Folgerung gilt für jedes nicht-negative $r \in \mathbb{Q}$ mit $a + r \in M$. Für $r \geq 0$ erhalten wir also

$$a + r \in M \Rightarrow a + (r - \frac{1}{k^2}) \in M.$$

Wiederholen wir den Prozess mit r ersetzt durch $r - \frac{1}{k^2}$, so erhalten wir nach endlich vielen Schritten $a + r_0 \in M$ für ein $r_0 \leq 0$. Addieren wir nun $-r_0$, so folgt $a \in M$. □

4.3 Archimedische quadratische Moduln von $\mathbb{R}[X_1, \ldots, X_n]$

Wir betrachten jetzt den Polynomring $A = \mathbb{R}[X_1, \ldots, X_n]$. Wie in Kapitel 3 seien für $h_1, \ldots, h_s \in A$ die folgenden Mengen definiert:

$$\begin{array}{rcl} W(h) & = & W(h_1, \ldots, h_s) = \{a \in \mathbb{R}^n \mid h_1(a) \geq 0, \ldots, h_s(a) \geq 0\} \\ T(h) & = & T(h_1, \ldots, h_s) = \sum_\nu h_1^{\nu_1} \cdots h_s^{\nu_s} \sum A^2 \\ M(h) & = & M(h_1, \ldots, h_s) = \sum A^2 + h_1 \sum A^2 + \ldots + h_s \sum A^2 \end{array}$$

$W(h)$ ist eine abgeschlossene semialgebraische Teilmenge des $\mathbb{R}^n$. $T(h)$ ist die von $h_1, \ldots, h_s$ erzeugte Präordnung, falls $-1 \notin T(h)$. $M(h)$ ist der von $h_1, \ldots, h_s$ erzeugte quadratische Modul, falls $-1 \notin M(h)$. Mit diesen Bezeichnungen erhalten wir den

Satz 4.12. *Es sind äquivalent*

(1) $M(h)$ *ist archimedisch,*

(2) (a) $W(h)$ *ist kompakt und*
(b) für alle $f \in A$ *mit* $f > 0$ *auf* $W(h)$ *gilt* $f \in M(h)$*,*

(3) $N - \sum_{i=1}^n X_i^2 \in M(h)$ *für ein* $N \in \mathbb{N}$*,*

(4) $\sigma(N - \sum_{i=1}^n X_i^2) \in 1 + M(h)$ *für ein* $N \in \mathbb{N}$ *und ein* $\sigma \in \sum A^2$*,*

(5) $W(f)$ *ist kompakt für ein* $f \in M(h)$*.*

Beweis. (1) ⇒ (2): Da $M(h)$ archimedisch ist, gibt es ein $N \in \mathbb{N}$ mit $N - \sum X_i^2 \in M(h)$. Also liegt $W(h)$ in einer Kugel um 0 mit Radius $\sqrt{N}$. Dies zeigt (a).

Um (b) zu zeigen, gehen wir wie in Satz 3.52 von Schmüdgen vor, benutzen aber den Jacobischen Darstellungssatz 4.11.

Sei also $f > 0$ auf $W(h)$. Wir zeigen $\widehat{f} > 0$ auf $X_{M(h)}^{\max}$ und erhalten dann mit Satz 4.11, dass $f \in M(h)$ gilt. Für $P \in X_{M(h)}^{\max}$ gilt $\alpha_P(h_i) = h_i(a_1, \ldots, a_n) \geq 0$, wobei $a_j = \alpha_P(X_j) \in \mathbb{R}$ für $1 \leq j \leq n$ ist. Also gilt

$$a = (a_1, \ldots, a_n) \in W(h).$$

Dann folgt aber

$$\widehat{f}(P) = \alpha_P(f) = f(a) > 0.$$

(2) $\Rightarrow$ (3): Wegen (a) gibt es ein $N \in \mathbb{N}$, so dass $N - \sum X_i^2 > 0$ auf $W(h)$ ist. Mit (b) folgt dann $N - \sum X_i^2 \in M(h)$.
(3) $\Rightarrow$ (4): Ist trivial, denn nach (3) ist mit $\sigma = 1$

$$\sigma(N + 1 - \sum X_i^2) \in 1 + M(h).$$

(4) $\Rightarrow$ (5): Falls $\sigma(N - \sum X_i^2) \in 1 + M(h)$ mit $\sigma \in \sum A^2$ gilt, so setze man $f = \sigma(N - \sum X_i^2) - 1$. Dann gilt $f \in M(h)$ und $W(f)$ ist selbstverständlich kompakt.
(5) $\Rightarrow$ (1): Ist $W(f)$ kompakt, so ist nach Satz 3.47, (2) $T(f)$ archimedisch. Wegen $f \in M(h)$ ist jedoch auch $T(f) \subseteq M(h)$. Also ist $M(h)$ archimedisch. □

In Satz 3.47, (2) hatten wir gesehen, dass $T(h)$ genau denn archimedisch ist, falls $W(h)$ kompakt ist. Für die Archimedizität des quadratischen Modul $M(h)$ ist die Kompaktheit von $W(h)$ zwar notwendig (vgl. (1) $\Rightarrow$ (2) in Satz 4.12), jedoch nicht mehr hinreichend. Dies hatten wir im Beispiel 3.53 gesehen. Wir wollen deshalb jetzt ein Kriterium erarbeiten, das tatsächlich auch hinreichend ist. Zuerst wollen wir jedoch einen speziellen Fall behandeln, bei dem die Kompaktheit von $W(h)$ doch noch hinreichend ist. Das ist der Fall, in dem alle h_i linear sind. Dazu erst ein einfaches Beispiel.

Beispiel 4.13. Es seien $h_1 = X_1, \ldots, h_n = X_n$ und $h_{n+1} = 1 - \sum_{i=1}^n X_i$. Selbstverständlich ist $W(h)$ kompakt.

Es gilt dann

$$1 - X_i = (1 - \sum X_i) + \sum_{j \neq i} X_j \in M(h)$$

und damit auch

$$1 - X_i^2 = \frac{1}{2}(1 + X_i)^2(1 - X_i) + \frac{1}{2}(1 - X_i)^2(1 + X_i) \in M(h).$$

Also ist $n - \sum X_i^2 \in M(h)$. Nach Satz 4.12 ist dann $M(h)$ archimedisch.

Um den allgemeinen Fall zu behandeln, zitieren wir den folgenden allgemein bekannten Satz von Minkowski.

Satz 4.14. *Seien $f, h_1 \ldots h_s \in \mathbb{R}[X_1, \ldots, X_n]$ lineare Polynome mit $W(h) := W(h_1, \ldots, h_s) \neq \emptyset$ und $f \geq 0$ auf $W(h)$. Dann existieren $\beta_0, \ldots, \beta_s \in \mathbb{R}^2$ mit*

$$f = \beta_0 + \beta_1 h_1 + \cdots + \beta_s h_s.$$

Als Folgerung daraus erhalten wir

Satz 4.15. *Seien* $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots X_n] = A$ *linear und sei* $W(h_1, \ldots h_s) \neq \emptyset$ *und kompakt. Dann ist* $M(h_1, \ldots, h_s)$ *archimedisch; also hat jedes* $f \in A$ *mit* $f > 0$ *auf* $W(h)$ *eine Darstellung*

$$f = \sigma_0 + \sigma_1 h_1 + \cdots + \sigma_s h_s$$

mit $\sigma_i \in \sum A^2$.

Beweis. Da $W(h)$ kompakt ist, sind für großes $N \in \mathbb{N}$ nach Satz 4.14 die linearen Polynome $N \pm X_i \in M(h)$. Dies hat zur Folge

$$N^2 - X_i^2 = \frac{1}{2N}(N + X_i)(N - X_i)^2 + \frac{1}{2N}(N - X_i)(N + X_i)^2 \in M(h).$$

Also auch $nN^2 - \sum X_i^2 \in M(h)$. Nach Satz 4.12 ist dann $M(h)$ archimedisch. □

Im Folgenden benutzen wir die Sprache der quadratischen Formen. Es sei F ein reeller Körper. Für $a_1, \ldots, a_m \in F$ bezeichnet

$$\varrho = \langle a_1, \ldots, a_m \rangle = a_1 Z_1^2 + \cdots + a_m Z_m^2$$

eine (diagonalisierte) *quadratische Form* über F. Sind alle $a_i \neq 0$, so heißt ϱ *regulär*. Weiter heißt ϱ *isotrop* über F, falls es $(z_1, \ldots z_m) \neq (0, \ldots, 0)$ im F^m mit $\sum a_i z_i^2 = 0$ gibt, d.h. die homogene Form ϱ stellt Null nicht-trivial dar. Man nennt ϱ *schwach isotrop*, falls es $\sigma_1, \ldots \sigma_m \in \sum F^2$ gibt, nicht alle Null, so dass

$$\sum_{i=1}^{n} a_i \sigma_i = 0$$

ist. Ist eines der $a_i = 0$, so ist ϱ selbstverständlich schwach isotrop. Man definiert deshalb mit

$$\varrho^* = \langle a_1, \ldots, a_m \rangle^*$$

den regulären Anteil von ϱ, d.h. man streicht diejenigen a_i, die Null sind. Ist mindestens ein $a_i \neq 0$, so bedeutet die schwache Isotropie von ϱ^* gerade, dass es $\sigma_1, \ldots \sigma_m \in \sum F^2$ gibt mit $\sum_{i=1}^n a_i \sigma_i = 0$ und mindestens einen Summanden $a_i \sigma_i \neq 0$. Hieraus ersieht man, dass ϱ^* in F nicht schwach isotrop sein kann, falls es eine Semi-Ordnung S von F mit $a_1, \ldots, a_m \in S$ gibt.

Lemma 4.16. *Seien $h_1, \dots, h_s \in \mathbb{R}[X_1, \dots X_n] = A$, für die $M(h_1, \dots, h_s)$ ein quadratischer Modul von A ist, und sei $f \in A$. Es gilt genau dann $\sigma f \in 1 + M(h)$ für ein $\sigma \in \sum A^2$, wenn für alle reellen Primideale $\mathfrak{p}$ von A die quadratische Form $\langle 1/\mathfrak{p}, -f/\mathfrak{p}, h_1/\mathfrak{p}, \dots, h_s/\mathfrak{p}\rangle^*$ in $F_\mathfrak{p} = \operatorname{Quot} A/\mathfrak{p}$ schwach isotrop ist.*

Beweis. "$\Rightarrow$" Wir schreiben kurz $\overline{g} = g/\mathfrak{p}, \overline{A} = A/\mathfrak{p}$, usw. Aus $\sigma f = 1 + \sigma_0 + \sigma_1 h_1 + \dots + \sigma_s h_s$ mit $\sigma, \sigma_0, \dots, \sigma_s \in \sum A^2$ folgt sofort

$$\overline{0} = (\overline{1} + \overline{\sigma}_0) - \overline{\sigma}\overline{f} + \overline{\sigma}_1 h_1 + \dots + \overline{\sigma}_s h_s.$$

Also ist $\langle \overline{1}, -\overline{f}, \overline{h}_1, \dots, \overline{h}_s\rangle^*$ schwach isotrop in $F_\mathfrak{p}$.
"$\Leftarrow$" Wir schließen mittels Kontraposition. Falls $f \sum A^2 \cap 1 + M(h) = \emptyset$, so gilt

$$-1 \notin M - f \sum A^2 =: M_1.$$

Also ist M_1 ein quadratischer Modul von A und lässt sich deshalb mit Zorns Lemma zu einer Semi-Ordnung S von A maximalisieren. Es gilt dann $M - f \sum A^2 \subseteq S$. Weiter ist $\mathfrak{p} = S \cap -S$ ein reelles Primideal von A. Wir betrachten

$$\alpha_S : A \to A/\mathfrak{p}.$$

Für das Bild von S unter α_S gilt $\overline{S} \cap -\overline{S} = \{\overline{0}\}$. Also kann die Semi-Ordnung $\overline{S}$ von $\overline{A} = A/\mathfrak{p}$ auf den Quotientenkörper $F_\mathfrak{p}$ zu einer Semi-Ordnung S' fortgesetzt werden. Für diese Semi-Ordnung S' gilt dann

$$\overline{1}, -\overline{f}, \overline{h}_1, \dots, \overline{h}_s \in S'.$$

Dann kann aber die Form $\langle \overline{1}, -\overline{f}, \overline{h}_1, \dots, \overline{h}_s\rangle^*$ in $F_\mathfrak{p}$ nicht schwach isotrop sein. □

Zur Formulierung und zum Beweis des nächsten Satzes benötigen wir ein paar Begriffe und Fakten aus der Bewertungstheorie, die man u.a. in [2] und [1] nachlesen kann. Teilweise sind diese Begriffe auch schon in den Übungen (siehe Anhang) behandelt worden, weshalb wir in diesem Abschnitt nicht detailliert darauf eingehen wollen.

Wir erinnern daran, dass ein Teilring $\mathcal{O}$ eines Körpers F ein Bewertungsring ist, falls für alle $x \in K$ mit $x \notin \mathcal{O}$ stets $x^{-1} \in \mathcal{O}$ gilt. Jedem Bewertungsring lässt sich eine Bewertung

$$v_\mathcal{O} \colon F \to \Gamma \cup \{\infty\}$$

zuordnen, wobei Γ eine angeordnete abelsche Gruppe ist. Es gilt dann

$$\mathcal{O} = \{x \in F \mid v_{\mathcal{O}}(x) \geq 0\}.$$

$\mathcal{O}$ ist genau dann trivial, wenn $\mathcal{O} = F$. Dies ist äquivalent zu $v_{\mathcal{O}}(F^\times) = \{0\}$.
Wir benötigen die folgenden Fakten:

Fakt 1: Ist Γ eine Untergruppe der additiven Gruppe von $\mathbb{R}$, also $v\colon F \to \mathbb{R} \cup \{\infty\}$, so lässt sich der bewertete Körper (F, v) "komplettieren", d.h. es gibt einen Oberkörper $\widehat{F}$ und eine Fortsetzung von v zu $\widehat{v}$ auf $\widehat{F}$, so dass in dem bewerteten Körper $(\widehat{F}, \widehat{v})$ jede Cauchyfolge konvergiert und F in $\widehat{F}$ dicht ist. $(\widehat{F}, \widehat{v})$ heißt die *Komplettierung* von (F, v).

Fakt 2: Hat F endlichen Transzendenzgrad über $\mathbb{R}$ und ist $\mathcal{O}'$ ein nicht-trivialer Bewertungsring von F mit $\mathbb{R} \subseteq \mathcal{O}'$, so gibt es einen Oberring $\mathcal{O} \neq F$ von $\mathcal{O}'$, so dass die Wertegruppe Γ von $v_{\mathcal{O}}$ eine Untergruppe von $(\mathbb{R}, +)$ ist.

Fakt 3: Ist $v\colon F \to \mathbb{R} \cup \{\infty\}$ nicht-trivial und $v(\mathbb{Q}^\times) = \{0\}$, so ist in $\widehat{F}$ jedes Element $1 + a$ mit $\widehat{v}(a) > 0$ ein Quadrat.

Wir können jetzt den folgenden wichtigen Satz formulieren:

Satz 4.17. *Seien $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots X_n] = A$, für die $M(h_1, \ldots, h_s)$ ein quadratischer Modul von A ist, und sei $f \in A$. Es gilt genau dann $\sigma f \in 1 + M(h)$ für ein $\sigma \in \sum A^2$, wenn $f > 0$ auf $W(h)$ ist und für jedes reelle Primideal $\mathfrak{p}$ von A und jede nicht-triviale Bewertung $v\colon F_{\mathfrak{p}} \to \mathbb{R} \cup \{\infty\}$ des Quotientenkörpers $F_{\mathfrak{p}} = A/\mathfrak{p}$ mit reellem Restklassenkörper und mindestens einem $v(X_i/\mathfrak{p}) < 0$ die quadratische Form*

$$\varrho = \langle 1/\mathfrak{p}, -f/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p}\rangle^*$$

in der Komplettierung $(\widehat{F}_{\mathfrak{p}}, \widehat{v})$ von $(F_{\mathfrak{p}}, v)$ schwach isotrop ist.

Beweis. Die Existenz eines $\sigma \in \sum A^2$ mit $\sigma f \in 1 + M(h)$ ist nach Lemma 4.16 dazu äquivalent, dass die quadratische Form ϱ in jedem der Restklassenkörper $F_{\mathfrak{p}}$ schwach isotrop ist. Wir zeigen , dass dies zu den Bedingungen des Satzes 4.17 äquivalent ist.
Sei zuerst ϱ in allen Restklassenkörpern $F_{\mathfrak{p}}$ schwach isotrop. Ist $\mathfrak{p}$ ein maximales reelles Ideal, also von der Gestalt $\mathfrak{p} = (X_1 - a_1, \ldots, X_n - a_n)$ für gewisses

$a = (a_1, \ldots, a_n) \in \mathbb{R}^n$, so gilt wegen $A/\mathfrak{p} \cong \mathbb{R}$ für ϱ (beachte $g/\mathfrak{p} = g(a)$ für $g \in A$):

$$\varrho = \langle 1, -f(a), h_1(a), \ldots, h_s(a)\rangle^*.$$

Wegen $F_\mathfrak{p} = \mathbb{R}$ und $h_1(a), \ldots, h_s(a) \geq 0$ für $a \in W(h)$, muss dann $-f(a)$ strikt negativ sein, um eine (schwache) Isotropie von ϱ in $\mathbb{R}$ zu erlauben. Also ist $f > 0$ auf $W(h)$.

Die zweite Bedingung ist trivalerweise erfüllt, da die schwache Isotropie in $F_\mathfrak{p}$ sich auf jeden Oberkörper vererbt, also auch auf $\widehat{F}_\mathfrak{p}$.

Seien jetzt die beiden Bedingungen des Satzes erfüllt. Wir zeigen dann durch Induktion über den Transzendenzgrad $\mathrm{trdeg}_\mathbb{R} F_\mathfrak{p}$ von $F_\mathfrak{p}$ über $\mathbb{R}$, dass ϱ in $F_\mathfrak{p}$ schach isotrop ist.

Für $\mathrm{trdeg}_\mathbb{R} F_\mathfrak{p} = 0$ muss $F_\mathfrak{p}$ algebraisch über $\mathbb{R}$ sein. Da $\mathfrak{p}$ reell sein soll, ist $F_\mathfrak{p}$ reell, also $F_\mathfrak{p} = \mathbb{R}$. Insbesondere ist dann $X_j/\mathfrak{p} = a_j \in \mathbb{R}$ für $1 \leq j \leq n$ und $g/\mathfrak{p} = g(a)$ für $g \in A$ und $a = (a_1, \ldots, a_n)$. Damit bedeutet $f > 0$ auf $W(h)$ nichts anderes, als dass die quadratische Form

$$\varrho = \langle 1, -f(a), h_1(a), \ldots, h_s(a)\rangle^*$$

über $\mathbb{R}$ indefinit ist. Dann ist sie aber auch isotrop in $\mathbb{R} = F_\mathfrak{p}$.

Sei jetzt $\mathrm{trdeg}_\mathbb{R} F_\mathfrak{p} > 0$. Dann ist $F_\mathfrak{p}$ transzendent über $\mathbb{R}$. Wir nehmen an, ϱ wäre nicht schwach isotrop in $F_\mathfrak{p}$. Dann ist

$$M = M(-f/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p}) \subseteq F_\mathfrak{p}$$

aber ein quadratischer Modul von $F_\mathfrak{p}$. Sonst hätten wir nämlich $-1 \in M$, also

$$-1 = \sigma_0 - \sigma f/\mathfrak{p} + \sigma_1 h_1/\mathfrak{p} + \cdots + \sigma_s h_s/\mathfrak{p}$$

für gewisse $\sigma, \sigma_i \in \sum F_\mathfrak{p}^2$. Dann wäre aber ϱ schwach isotrop in $F_\mathfrak{p}$.

Nach Zorns Lemma gibt es über M eine Semi-Ordnung S von $F_\mathfrak{p}$, für die dann

$$-f/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p} \in S$$

gilt.

Wir bilden nun nach Satz 4.6 (und Zusatz 4.7) den Bewertungsring $\mathcal{O}(S) \subseteq F_\mathfrak{p}$. Dies ist bezüglich der Semiordnung $\leq_S$ von $F_\mathfrak{p}$ die konvexe Hülle von $\mathbb{Z}$ in $F_\mathfrak{p}$. Da $\leq_S$ eingeschränkt auf $\mathbb{R}$ die übliche Anordnung von $\mathbb{R}$ ist, ist der Körper $\mathbb{R}$ in $\mathcal{O}(S)$ enthalten. Weiter muss $\mathcal{O}(S) \neq F_\mathfrak{p}$ gelten, da sonst nach Satz 4.5 die Semi-Ordnung $\leq_S$ auf $F_\mathfrak{p}$ eine archimedische Anordnung wäre. Dann wäre aber $F_\mathfrak{p}$ in $\mathbb{R}$ einbettbar, also gleich $\mathbb{R}$.

Beachten wir nun, dass $F_\mathfrak{p}$ über $\mathbb{R}$ endlich erzeugt ist (nämlich von $X_1/\mathfrak{p}, \ldots, X_n/\mathfrak{p}$), so erhalten wir mit *Fakt 2* von oben einen Bewertungsring $\mathcal{O} \neq F_\mathfrak{p}$ von $F_\mathfrak{p}$ mit $\mathcal{O}(S) \subseteq \mathcal{O}$ und der zugehörigen nicht-trivialen Bewertung

$$v_\mathcal{O} : F_\mathfrak{p} \to \mathbb{R} \cup \{\infty\}.$$

Wie wir sehen werden, induziert die Semi-Ordnung S dann zum einen eine Semi-Ordnung $\overline{S} = \varrho(S \cap \mathcal{O})$ des Restklassenkörpers $k = \mathcal{O}/\mathcal{M}$, wobei $\varrho(a) = a + \mathcal{M}$ der Restklassenhomomorphismus ist, und zum anderen eine Semi-Ordnung $\widehat{S}$ der nach *Fakt 1* existierenden Komplettierung $\widehat{F}_\mathfrak{p}$ von $F_\mathfrak{p}$ bezüglich der Bewertung $v_\mathcal{O}$.

Wir betrachten zuerst $\overline{S}$. Die Inklusionen $\overline{S} + \overline{S} \subseteq \overline{S}$ und $\overline{S}k^2 \subseteq \overline{S}$ sowie $\overline{S} \cup -\overline{S} = k$ sind klar. Es bleibt lediglich $-1 \notin \overline{S}$ zu zeigen. Falls $-1 \equiv s \mod \mathcal{M}$ für ein $s \in S$ wäre, so hätten wir $1 + s \in \mathcal{M}$. Wegen $\mathcal{O}(S) \subseteq \mathcal{O}$ gilt aber $\mathcal{M} \subseteq \mathcal{M}(S)$. Also gilt $1 + s \in \mathcal{M}(S)$. Dies ist jedoch unmöglich, da $\mathcal{M}(S)$ konvex ist: es wäre dann $-1 \in \mathcal{M}(S)$. Insbesondere ist der Restklassenkörper k von $v_\mathcal{O}$ reell, da er eine Semi-Ordnung besitzt.

Als nächstes betrachten wir den topologischen Abschluss $\widehat{S}$ von S in $\widehat{F}_\mathfrak{p}$. Wiederum sind die Inklusionen $\widehat{S} + \widehat{S} \subseteq \widehat{S}$ und $\widehat{S}(\widehat{F}_\mathfrak{p})^2 \subseteq \widehat{S}$ sowie $\widehat{S} \cup -\widehat{S} = \widehat{F}_\mathfrak{p}$ klar. Es bleibt $-1 \notin \widehat{S}$ zu zeigen. Wäre -1 Häufungspunkt von Elementen aus S, so gäbe es ein $s \in S$, so dass s in der offenen Umgebung $-1 + \mathcal{M}$ von -1 liegen würde. Dann wäre wieder $s + 1 \in \mathcal{M}$, ein Widerspruch wie vorhin.

Nun unterscheiden wir zwei Fälle:

1. Fall: Ein $X_i/\mathfrak{p}$ liegt nicht in $\mathcal{O}$, d.h. $v_\mathcal{O}(X_i/\mathfrak{p}) < 0$. In diesem Fall müsste dann nach Voraussetzung die quadratische Form ϱ in $\widehat{F}_\mathfrak{p}$ schwach isotrop sein. Dies ist jedoch nicht möglich, da alle Elemente

$$-f/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p}$$

in der Semi-Ordnung $\widehat{S}$ von $\widehat{F}_\mathfrak{p}$ liegen.

2. Fall: Alle $X_i/\mathfrak{p}$ liegen in $\mathcal{O}$. Dann liegt auch ganz $A/\mathfrak{p}$ in $\mathcal{O}$. Der Restklassenhomomorphismus $\varrho\colon \mathcal{O} \to k$ hat einen nicht-trivialen Kern in $A/\mathfrak{p}$. Sonst wären alle Elemente von $A/\mathfrak{p} \setminus \{0\}$ Einheiten in $\mathcal{O}$. Also wäre Quot $A/\mathfrak{p}$ in $\mathcal{O}$, d.h. $\mathcal{O}$ wäre gleich $F_\mathfrak{p}$, ein Widerspruch. Die Komposition der Homomorphismen

$$\alpha\colon A \to A/\mathfrak{p} \xrightarrow{\varrho} k$$

hat als Kern ein Primideal $\mathfrak{q} \supsetneq \mathfrak{p}$. Also gilt für $F_\mathfrak{q} = \text{Quot } A/\mathfrak{q}$

$$\text{trdeg}_\mathbb{R} F_\mathfrak{q} < \text{trdeg}_\mathbb{R} F_\mathfrak{p}.$$

Da $\mathfrak{q}$ reell ist (beachte $F_{\mathfrak{q}} \subseteq k$), wissen wir nach Induktionsvoraussetzung, dass ϱ in $F_{\mathfrak{q}}$ schwach isotrop ist. Dies ist jedoch unmöglich, da $\overline{S}$ eine Semi-Ordnung von k mit der Eigenschaft

$$-f/\mathfrak{q}, h_1/\mathfrak{q}, \ldots, h_s/\mathfrak{q} \in \overline{S}$$

ist.

Insgesamt haben wir damit einen Widerspruch zu der Annahme ϱ sei in $F_{\mathfrak{p}}$ nicht schwach isotrop erzielt. Also ist ϱ doch schwach isotrop in $F_{\mathfrak{p}}$. □

Wir können nun die Archimedizität von quadratischen Moduln des Polynomringes $\mathbb{R}[X_1, \ldots, X_n]$ charakterisieren.

Charakterisierungssatz 4.18. *Seien $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots X_n] = A$, für die $M(h_1, \ldots, h_s)$ ein quadratischer Modul von A ist. $M(h)$ ist genau dann archimedisch, wenn $W(h)$ kompakt ist, und wenn für jedes reelle Primideal $\mathfrak{p}$ von A und jede nicht-triviale Bewertung $v\colon F_{\mathfrak{p}} \to \mathbb{R} \cup \{\infty\}$ mit reellem Restklassenkörper und mindestens einem $v(X_i/\mathfrak{p}) < 0$ (dabei ist $F_{\mathfrak{p}} = \operatorname{Quot} A/\mathfrak{p}$), die quadratische Form*

$$\tau = \langle 1/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p}\rangle^*$$

in der Komplettierung $(\widehat{F}_{\mathfrak{p}}, \widehat{v})$ von $(F_{\mathfrak{p}}, v)$ schwach isotrop ist.

Beweis. "⇒" Ist $M(h_1, \ldots, h_s)$ archimedisch, dann gibt es ein $N \in \mathbb{N}$ mit $N - \sum X_i^2 \in 1 + M(h)$. Setzen wir $f := N - \sum X_i^2$, so liefert Satz 4.17, dass $f > 0$ auf $W(h)$ ist (also ist $W(h)$ kompakt), und dass für die betrachteten Primideal $\mathfrak{p}$ die quadratische Form

$$\varrho = \langle 1/\mathfrak{p}, -f/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p}\rangle^*$$

in $\widehat{F}_{\mathfrak{p}}$ schwach isotrop ist.

Sei in der betrachteten Situation etwa $v(X_1/\mathfrak{p}) < 0$. Dann schreiben wir

$$-f = X_1^2(1 - \frac{N}{X_1^2}) + X_2^2 + \cdots + X_n^2.$$

Da der Restklassenkörper von v reell ist, muss N eine Einheit in $\mathcal{O}$ sein. Damit liegt $\frac{N}{X_1^2}$ aber im maximalen Ideal von $\mathcal{O}$, also ist $v(\frac{N}{X_1^2}) > 0$. Mit *Fakt 3* erhalten wir dann, dass $1 - \frac{N}{X_1^2}$ ein Quadrat in $\widehat{F}_{\mathfrak{p}}$ ist. Also ist $-f$ eine

Quadratsumme in $\widehat{F}_\mathfrak{p}$. Somit folgt aus der schachen Isotropie von ϱ diejenige von τ in $\widehat{F}_\mathfrak{p}$.

"$\Leftarrow$" Da $W(h)$ kompakt ist, gibt es $N \in \mathbb{N}$, so dass $f := N - \sum X_i^2$ strikt positiv auf $W(h)$ ist. Die schwache Isotropie der quadratischen Form τ in $\widehat{F}_\mathfrak{p}$ impliziert trivialerweise diejenige von $\varrho = \langle 1, -f/\mathfrak{p}, h_1/\mathfrak{p}, \ldots, h_s/\mathfrak{p}\rangle^*$.
Damit erhalten wir aus Satz 4.17 die Existenz von $\sigma \in \sum A^2$ mit $\sigma f \in 1 + M(h)$. Dann folgt aber mit Satz 4.12 die Archimedizität von $M(h)$. □

Zum Abschluss dieses Kapitels bringen wir noch einen Fall, in dem die Kompaktheit von $W(h)$ hinreichend für die Archimedizität von $M(h)$ ist. Dabei verwenden wir im Beweis einige Fakten aus der Theorie der quadratischen Formen über Körpern, die man ohne weiteres in der Standardliteratur findet.

Satz 4.19. *Es seien* $h_1, h_2 \in \mathbb{R}[X_1, \ldots, X_n] = A$*, für die* $M(h_1, h_2)$ *ein quadratischer Modul von* A *ist. Ist* $W(h_1, h_2)$ *kompakt, so ist* $M(h_1, h_2)$ *archimedisch.*

Beweis. Nach Satz 3.47 folgt aus der Kompaktheit von $W(h_1, h_2)$ die Archimedizität der Präordnung

$$T(h_1, h_2) = M(h_1, h_2, h_1h_2).$$

Mit Satz 4.18 folgt dann aus der Archimedizität von $M(h_1, h_2, h_1h_2)$ die schwache Isotropie der quadratischen Form

$$\tau = \langle 1, \overline{h}_1, \overline{h}_2, \overline{h}_1\overline{h}_2\rangle^*$$

in den dort betrachteten Komplettierungen $\widehat{F}_\mathfrak{p}$. (Wir schreiben kurz $\overline{g}$ für $g/\mathfrak{p}$.) Wir werden hieraus die schwache Isotropie von $\langle 1, \overline{h}_1, \overline{h}_2\rangle^*$ folgern und erhalten dann wieder mit Satz 4.18 die Archimedizität von $M(h_1, h_2)$.

Ist $\overline{h}_1 = 0$ oder $\overline{h}_2 = 0$, so ist nichts zu zeigen. Es bleibt der Fall $\overline{h}_1 \neq 0 \neq \overline{h}_2$.

Benutzt man nun die in der Theorie der quadratischen Formen übliche Definition eines Produktes

$$\langle a_1, \ldots, a_m\rangle \otimes \langle b_1, \ldots, b_k\rangle := \langle a_1b_1, \ldots, a_mb_1, a_1b_2, \ldots, a_mb_2, \ldots, a_mb_k\rangle,$$

so erkennt man, dass die schwache Isotropie von τ gerade die Isotropie eines $m+2$-fachen Produktes

$$\sigma_1 = \langle 1,1\rangle \otimes \cdots \otimes \langle 1,1\rangle \otimes \langle 1,\overline{h}_1\rangle \otimes \langle 1,\overline{h}_2\rangle$$

ist. Ein solches Produkt ist eine sogenannte Pfisterform und hat die Eigenschaft, dass aus ihrer Isotropie die Isometrie zu jedem Produkt der Gestalt

$$\sigma_2 = \langle 1,1\rangle \otimes \cdots \otimes \langle 1,1\rangle \otimes \langle -a_{m+1}, a_{m+1}\rangle \otimes \langle -a_{m+2}, a_{m+2}\rangle$$

mit $a_i \neq 0$ folgt. Dabei können die a_i beliebig ($\neq 0$) gewählt werden. Wir wählen $a_{m+2} = \overline{h}_1\overline{h}_2$ und $a_{m+1} = 1$.

Multipliziert man nun die Produkte σ_1 und σ_2 aus, so erkennt man, dass das Produkt $\overline{h}_1\overline{h}_2$ in beiden Formen 2^m-mal auftaucht. Nach dem Wittschen Kürzungssatz können diese gleichen Einträge gestrichen werden und man erhält die Isometrie der Form

$$\langle 1,1\rangle \otimes \cdots \otimes \langle 1,1\rangle \otimes \langle 1,\overline{h}_1,\overline{h}_2\rangle$$

mit der Form

$$\langle 1,1\rangle \otimes \cdots \otimes \langle 1,1\rangle \otimes \langle -1,1,-\overline{h}_1\overline{h}_2\rangle.$$

Damit ist die schwache Isotropie von $\langle 1,\overline{h}_1,\overline{h}_2\rangle$ in $\widehat{F}_{\mathfrak{p}}$ nachgewiesen. $\square$

A Übungsaufgaben

Übungsblatt 1

Definition 1. Ein angeordneter Körper $(K, \leq)$ heißt

(i) *schnittvollständig* (oder *Dedekind-vollständig*), wenn es zu je zwei nichtleeren Teilmengen A, B von K mit $A \leq B$ (d.h. $a \leq b$ für alle $a \in A$ und alle $b \in B$) stets ein $c \in K$ mit $A \leq c \leq B$ gibt.

(ii) *archimedisch*, wenn zu jedem $a \in K$ ein $n \in \mathbb{N}$ mit $a \leq n$ existiert.

(iii) *vollständig*, wenn jede Cauchy-Folge in K konvergiert.

Aufgabe 1.1. Sei $(K, \leq)$ ein angeordneter Körper. Zeigen Sie, dass $(K, \leq)$ genau dann schnittvollständig ist, wenn er archimedisch und vollständig ist.

Aufgabe 1.2. Sei $(K, \leq)$ ein archimedisch angeordneter Körper und $\rho\colon K \to \mathbb{R}$ die Abbildung, die jedem Element $a \in K$ die eindeutig bestimmte reelle Zahl $\rho(a) \in \mathbb{R}$ mit $U_a \leq \rho(a) \leq O_a$ zuordnet, wobei

$$U_a := \{s \in \mathbb{Q} \mid s < a\} \text{ und } O_a := \{r \in \mathbb{Q} \mid a \leq r\}.$$

Zeigen Sie:

a) ρ ist ein Ringhomomorphismus, also eine Körpereinbettung.

b) Für alle $a, b \in K$ gilt

$$a \leq b \iff \rho(a) \leq \rho(b).$$

Insbesondere ist ρ ordnungstreu.

Aufgabe 1.3. Sei $(K, \leq)$ ein archimedisch angeordneter Körper. Zeigen Sie, dass der einzige ordnungstreue Automorphismus von $(K, \leq)$ die Identitätsabbildung ist.

Definition 2. Sei $G := (G, \cdot)$ eine Gruppe. Eine lineare Ordnung $\leq$ auf der Menge G heißt eine *Anordnung* von G, wenn für alle $g_1, g_2, h \in G$ folgendes gilt:

$$g_1 \leq g_2 \Rightarrow g_1 \cdot h \leq g_2 \cdot h \text{ und } h \cdot g_1 \leq h \cdot g_2.$$

Man nennt dann $(G, \leq)$ eine *angeordnete Gruppe*.

Aufgabe 1.4. Sei $(G, \leq)$ eine angeordnete Gruppe, und sei N ein Normalteiler von G. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) N ist *konvex* bezüglich $\leq$, d.h. für alle $g_1, g_2 \in N$ und $h \in G$ gilt:

$$g_1 \leq h \leq g_2 \Rightarrow h \in N.$$

(ii) Durch

$$g_1 N \preceq g_2 N : \Longleftrightarrow \ g_1 \leq g_2 \text{ oder } g_1 N = g_2 N$$

für $g_1, g_2 \in G$ wird auf G/N eine Anordnung definiert.

Übungsblatt 2

Definition / Erinnerung 3. Ein Integritätsbereich $\mathcal{O}$ mit Quotientenkörper K heißt *Bewertungsring* von K, wenn für alle $x \in K^\times$ stets $x \in \mathcal{O}$ oder $x^{-1} \in \mathcal{O}$ gilt.

Überlegen (bzw. Erinnern) Sie sich, dass Bewertungsringe ganz abgeschlossene lokale Ringe sind. Erinnern Sie sich an die Eigenschaften ganz abgeschlossener Ringe.

Sei $\mathcal{O}$ ein Bewertungsring eines Körpers K, und sei $\mathfrak{m}$ sein einziges maximales Ideal. Dann heißt $\overline{K} := \mathcal{O}/\mathfrak{m}$ der *Restklassenkörper* von $\mathcal{O}$.

Aufgabe 2.1. Sei $(K, \leq)$ ein angeordneter Körper, und sei $P := P_\leq$ der Positivbereich zu $\leq$.

Sei $\mathcal{O}$ ein Teilring von K, der *konvex* bezüglich der Anordnung $\leq$ ist, d.h. für alle $x \in \mathcal{O}$ und $y \in K$ gilt:

$$0 \leq y \leq x \Rightarrow y \in \mathcal{O}.$$

Zeigen Sie, dass $\mathcal{O}$ ein Bewertungsring von K ist.

Sei nun $\mathcal{O}$ ein beliebiger Bewertungsring von K mit maximalem Ideal $\mathfrak{m}$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) $\mathcal{O}$ ist konvex bezüglich $\leq$.

(ii) $\mathfrak{m}$ ist als Untergruppe der additiven Gruppe von $\mathcal{O}$ konvex bezüglich $\leq$.

(iii) Auf dem Restklassenkörper $\overline{K} = \mathcal{O}/\mathfrak{m}$ von $\mathcal{O}$ wird durch

$$x + \mathfrak{m} \preceq y + \mathfrak{m} : \Longleftrightarrow \ x \leq y \text{ oder } x \equiv y \bmod \mathfrak{m}$$

für $x, y \in \mathcal{O}$ eine Anordnung mit Positivbereich $\overline{P} = \{p + \mathfrak{m} \mid p \in P \cap \mathcal{O}\}$ definiert.

(iv) $1 + \mathfrak{m} \subseteq P$.

Definition 4. Seien K ein Körper und Γ eine angeordnete abelsche Gruppe. Eine Abbildung $v\colon K \to \Gamma \cup \{\infty\}$ heißt *Bewertung* von K, falls die folgenden Bedingungen für alle $x, y \in K$ gelten:

(i) $v(x) = \infty \iff x = 0$,

(ii) $v(xy) = v(x) + v(y)$,

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Dabei ist stets $\infty + \gamma = \gamma + \infty = \infty$ für alle $\gamma \in \Gamma \cup \{\infty\}$ und $\gamma < \infty$ für alle $\gamma \in \Gamma$.
Gilt zusätzlich $v(K^\times) = \Gamma$, so heißt Γ die *Wertegruppe* von v.

Aufgabe 2.2. Sei K ein Körper. Zeigen Sie:

a) Sei $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$ eine Bewertung von K. Dann ist $\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ ein Bewertungsring von K mit maximalem Ideal $\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$.

b) Sei $\mathcal{O}$ ein Bewertungsring von K. Dann wird durch

$$x\mathcal{O}^\times \leq y\mathcal{O}^\times :\iff yx^{-1} \in \mathcal{O}$$

auf der abelschen Gruppe $\Gamma_\mathcal{O} := K^\times/\mathcal{O}^\times$ bezüglich der additiv geschriebenen Gruppenoperation $x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times$ eine Anordnung definiert.
Die Restklassenabbildung

$$\begin{aligned} v_\mathcal{O}\colon K^\times &\twoheadrightarrow \Gamma_\mathcal{O} \\ x &\mapsto x\mathcal{O}^\times \end{aligned}$$

induziert eine Bewertung von K mit Wertegruppe $\Gamma_\mathcal{O}$ und Bewertungsring $\mathcal{O}_{v_\mathcal{O}} = \mathcal{O}$.

c) Sei $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$ eine Bewertung von K. Dann wird durch

$$\begin{aligned} K^\times/\mathcal{O}_v^\times &\to \Gamma \\ x\mathcal{O}_v^\times &\mapsto v(x) \end{aligned}$$

ein ordnungstreuer Isomorphismus der Wertegruppen von $v_{\mathcal{O}_v}$ und v definiert.

Aufgabe 2.3. Sei v eine Bewertung eines Körpers K und $\mathcal{O}_v$ der zugehörige Bewertungsring. Zeigen Sie:

a) Der Restklassenkörper $\overline{K}$ von $\mathcal{O}_v$ ist genau dann reell, wenn für alle $a_1, \ldots, a_n \in K$ folgendes gilt:

$$v(a_1^2 + \cdots + a_n^2) = \min\{v(a_i^2) \mid 1 \leq i \leq n\}.$$

b) Ist $\overline{K}$ reell, so gibt es eine Anordnung von K, bezüglich der $\mathcal{O}$ konvex ist.
(Hinweis: Konstruieren Sie zuerst aus einem Positivbereich von $\overline{K}$ einen Präpositivbereich von K.)

Aufgabe 2.4. Sei R ein reell abgeschlossener Körper, sei $\mathcal{O}$ ein (bezüglich der einzigen Anordnung von R) konvexer Bewertungsring von R. Zeigen Sie:

a) Der Restklassenkörper $\overline{R}$ von $\mathcal{O}$ ist ebenfalls reell abgeschlossen.

b) Die Wertegruppe $\Gamma_{\mathcal{O}}$ von $\mathcal{O}$ ist *divisibel*, d.h. zu jedem $\gamma \in \Gamma_{\mathcal{O}}$ und jedem $n \in \mathbb{N} \setminus \{0\}$ existiert ein $\gamma' \in \Gamma_{\mathcal{O}}$ mit $\gamma = n\gamma'$.

c) $(R, \mathcal{O})$ ist ein *henselsch* bewerteter Körper, d.h. für alle normierten Polynome $f \in \mathcal{O}[X]$ (X eine Unbestimmte) gilt: Wenn $\overline{f}$ eine einfache Nullstelle $\overline{a} \in \overline{R}$ hat, so besitzt f eine Nullstelle $b \in \mathcal{O}$ mit $\overline{b} = \overline{a}$.
Hierbei bezeichne $\overline{f}$ das Polynom $X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_0} \in \overline{R}[X]$, wenn $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ mit $a_i \in \mathcal{O}$ $(1 \leq i \leq n-1)$ ist.
(Hinweis: Zeigen Sie die Aussage zuerst für alle normierten Polynome aus $\mathcal{O}[X]$ vom Grad ≤ 2 und erinnern Sie sich dann an den Fundamentalsatz der Algebra.)

Übungsblatt 3

Aufgabe 3.1. Sei $K = \mathbb{R}(t)$ der rationale Funktionenkörper in einer Unbestimmten t über $\mathbb{R}$, und sei $\leq$ die (eindeutig bestimmte) Anordnung von K, für welche $0 < t < \frac{1}{n}$ für alle $n \in \mathbb{N} \setminus \{0\}$ ist. Sei $(R, \leq)$ der reelle Abschluß von $(K, \leq)$. Zeigen Sie:

a) K ist nicht dicht in R. Es gibt z.B. kein $a \in K$ mit $\sqrt{t} < a < 2\sqrt{t}$.

b) Das Polynom $f = X^4 - 5tX^2 + 4t^2$ nimmt über K nur positive Werte an, über R jedoch auch negative Werte.

Aufgabe 3.2. Sei K ein Körper, und seien

$$K[[X]] := \left\{ \sum_{i=0}^{\infty} a_i X^i \mid a_i \in \mathbb{R} \ (i \geq 0) \right\}$$

die Menge der formalen Potenzreihen und

$$K((X)) := \left\{ \sum_{i=m}^{\infty} a_i X^i \mid m \in \mathbb{Z},\ a_i \in \mathbb{R} \ (i \geq m) \right\}$$

die Menge der formalen Laurentreihen in einer Unbestimmten über K.
Dabei identifizieren wir stets $\sum_{i=m}^{\infty} a_i X^i$ mit $0X^{m-1} + \sum_{i=m}^{\infty} a_i X^i$.
Zusammen mit der Addition

$$\sum_{i=m}^{\infty} a_i X^i + \sum_{i=m}^{\infty} b_i X^i := \sum_{i=m}^{\infty} (a_i + b_i) X^i$$

und der Multiplikation

$$\left(\sum_{i=m}^{\infty} a_i X^i \right) \cdot \left(\sum_{i=m}^{\infty} b_i X^i \right) := \sum_{i=m}^{\infty} \Big(\sum_{j+k=i} a_j b_k \Big) X^i$$

sind $K[[X]]$ und $K((X))$ Integritätsbereiche.
Zeigen Sie:

a) Es gilt $\sum_{i=0}^{\infty} a_i X^i \in K[[X]]^\times$ genau dann, wenn $a_0 \neq 0$.

b) $K((X)) = \mathrm{Quot}(K[[X]])$, insbesondere ist $K((X))$ ein Körper.

c) $K[[X]]$ ist ein Bewertungsring von $K((X))$. Bestimmen Sie außerdem das maximale Ideal, den Restklassenkörper und die Wertegruppe von $K[[X]]$.

d) Sei $K = \mathbb{R}$. Der Körper $\mathbb{R}((X))$ besitzt genau zwei Anordnungen. (Hinweis: Potenzreihen der Form $1+\sum_{i=1}^{\infty} a_i X^i$ sind Quadrate in $\mathbb{R}((X))$.)

Aufgabe 3.3. Sei C ein algebraisch abgeschlossener Körper der Charakteristik 0. Zeigen Sie, dass C einen reell abgeschlossenen Teilkörper R mit $C = R(\sqrt{-1})$ besitzt.

Aufgabe 3.4. Sei K ein angeordneter Körper. Zeigen Sie:

a) Das System aller Mengen

$$]a, b[:= \{x \in K \mid a < x < b\} \qquad (a, b \in K)$$

überdeckt ganz K und ist abgeschlossen unter endlichen Durchschnitten.
Insbesondere bildet dieses System die Basis einer Topologie auf K, der sogenannten *Intervalltopologie*.

b) Bezüglich der Intervalltopologie sind die beiden Körperoperationen als Abbildungen von $K \times K$, ausgestattet mit der Produkttopologie, nach K und das Invertieren als Abbildung von $K^\times$, ausgestattet mit der Spurtopologie, nach K stetig.

c) K ist bezüglich der Intervalltopologie genau dann ein zusammenhängender topologischer Raum, wenn K schnittvollständig (also $K \cong \mathbb{R}$) ist.

d) Sei $K = R$ ein reell abgeschlossener Körper. Dann stimmt auf R^n die von der euklidischen Norm

$$\|\cdot\| \colon R^n \to R,\ (x_1, \ldots, x_n) \mapsto \sqrt{x_1^2 + \cdots + x_n^2}$$

induzierte Topologie mit der Produkttopologie der Intervalltopologie auf R überein.

Übungsblatt 4

Aufgabe 4.1. Zeigen Sie, dass die aufgeschlitzte Kreisscheibe

$$\{re^{i\varphi} \mid 0 < r < 1, 0 < \varphi < 2\pi\} \subseteq \mathbb{C} = \mathbb{R}^2$$

keine basisoffene semialgebraische Menge ist, sehr wohl aber Vereinigung zweier solcher.

Aufgabe 4.2. Sei R ein reell abgeschlossener Körper. Zeigen Sie, dass es kein Polynom $f \in R[X, Y]$ gibt, so dass

$$\{(x, y) \in R^2 \mid x > 0, y > 0\} = \{(x, y) \in R^2 \mid f(x, y) > 0\}.$$

(Hinweis: Schreiben Sie f als $X^n Y^m g$ so, dass weder X noch Y das Polynom g teilen.)

Aufgabe 4.3. Sei $S \subseteq R^n$ eine semialgebraische Menge über einem reell abgeschlossenen Körper R. Sei $f\colon S \to R^m$ eine *semialgebraische Funktion*, d.h. der Graph von f

$$\Gamma(f) = \{(x, f(x)) \in R^{n+m} \mid x \in S\}$$

ist semialgebraisch. Zeigen Sie, dass für jede semialgebraische Teilmenge S' von S auch $f(S') \subseteq R^m$ wieder semialgebraisch ist.

Definition 5. Ein angeordneter Körper $(K, \leq)$ heißt η_1-*angeordnet*, wenn es zu je zwei abzählbaren Mengen $A, B \subseteq K$ mit $A < B$ stets ein $c \in K$ mit $A < c < B$ gibt.

Aufgabe 4.4. Sei $(K, \leq)$ ein η_1-angeordneter Körper. Zeigen Sie:

a) K ist überabzählbar und $(K, \leq)$ ist nicht archimedisch.

b) Ist K zusätzlich reell abgeschlossen, so läßt sich jeder abzählbare, angeordnete Körper ordnungstreu in K einbetten.
(Hinweis: Sei $F = \{x_1, x_2, \ldots\}$ ein abzählbarer, angeordneter Körper und R sein reeller Abschluß. Betrachten Sie die Kette:

$$\overline{\mathbb{Q}} \subseteq \overline{\overline{\mathbb{Q}}(x_1)} \subseteq \overline{\overline{\overline{\mathbb{Q}}(x_1)}(x_2)} \subseteq \cdots .$$

(Zu einem Körper $L \subseteq R$ bezeichne $\overline{L}$ seinen relativ algebraischen Abschluß in R.))

Übungsblatt 5

Aufgabe 5.1. Sei $S \subseteq R^n$ eine semialgebraische Menge über einem reell abgeschlossenen Körper R. Wir bezeichnen mit $\overline{S}$ den *Abschluß* von S in der euklidischen Topologie auf dem R^n (vgl. Aufgabe 3.4). Außerdem bezeichnen wir mit $S^\circ := R^n \setminus (\overline{R^n \setminus S})$ das *Innere* und mit $\overline{S} \setminus S^\circ$ den *Rand* von S. Zeigen Sie, dass der Abschluß, das Innere und der Rand von S wieder semialgebraisch sind.

Aufgabe 5.2. Beschreiben Sie für jede natürliche Zahl $n \geq 3$ das Innere eines regelmäßigen n-Ecks im $\mathbb{R}^2$ durch zwei strikte polynomiale Ungleichungen.

Aufgabe 5.3. Zeigen Sie, dass das Polynom

$$f(X,Y) = X^2Y^2(X^2 + Y^2 - 3) + 1 \in \mathbb{R}[X,Y]$$

auf ganz $\mathbb{R}^2$ nur nichtnegative Werte animmt, sich aber nicht als Summe von Polynomquadraten darstellen lässt.
(Hinweis: Zeigen Sie zuerst für $a, b, c \in \mathbb{R}$ mit $a, b, c \geq 0$ die Ungleichung $(a+b+c)^3 \geq 9abc$.)

Aufgabe 5.4. Sei $(K, \leq)$ ein angeordneter Körper. Sei $\mathcal{O}$ die konvexe Hülle von $\mathbb{Q}$ in K bezüglich $\leq$, d.h.

$$\mathcal{O} = \{x \in K \mid \exists r \in \mathbb{Q} \text{ mit } |x| \leq r\}.$$

Nach Aufgabe 2.1 ist $\mathcal{O}$ ein Bewertungsring von K. Sei $\mathfrak{m}$ das maximale Ideal von $\mathcal{O}$ und $\overline{K} = \mathcal{O}/\mathfrak{m}$ sein Restklassenkörper. Wir wissen aus Aufgabe 2.1 ebenfalls, dass $\leq$ eine Anordnung $\preceq$ auf $\overline{K}$ induziert. Zeigen Sie:

a) $(\overline{K}, \preceq)$ ist archimedisch.

b) Ist $(K, \leq)$ η_1-angeordnet, so ist $(\overline{K}, \preceq)$ schnittvollständig, also insbesondere $\overline{K} \cong \mathbb{R}$.

Übungsblatt 6

Aufgabe 6.1. Finden Sie $m, n \in \mathbb{N}$ und $g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$, so dass das Innere der semialgebraischen Menge

$$\{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

nicht durch

$$\{x \in \mathbb{R}^n \mid g_1(x) > 0, \ldots, g_m(x) > 0\}$$

gegeben ist.

Definition 6. Sei $S \subseteq R^n$ eine semialgebraische Menge über einem reell abgeschlossenen Körper R. Dann heißt S *semialgebraisch zusammenhängend*, wenn es keine zwei in S abgeschlossenen semialgebraischen Mengen $\emptyset \subsetneq S_1, S_2 \subseteq S$ mit $S_1 \cap S_2 = \emptyset$ und $S = S_1 \cup S_2$ gibt.

Aufgabe 6.2. Sei R ein reell abgeschlossener Körper.

a) Bestimmen Sie alle semialgebraischen Teilmengen von R. Welche davon sind semialgebraisch zusammenhängend?

b) Sei $n \in \mathbb{N}$. Zeigen Sie, dass der offene Hyperwürfel $]0, 1[^n \subseteq R^n$ semialgebraisch zusammenhängend ist.

Aufgabe 6.3. Für $n \in \mathbb{N}$ sei das Polynom

$$f_n := \sum_{i=1}^{n} \prod_{j \neq i} (X_i - X_j) \in \mathbb{R}[X_1, \ldots, X_n]$$

gegeben. Für welche $n \in \mathbb{N}$ ist

a) $f_n \geq 0$ auf dem $\mathbb{R}^n$?

b) f_n eine Quadratsumme in $\mathbb{R}[X_1, \ldots, X_n]$?

Aufgabe 6.4. Sei $(K, \mathcal{O})$ ein henselsch bewerteter Körper. Zeigen Sie, dass $\mathcal{O}$ bezüglich jeder Anordnung von K konvex ist.

Übungsblatt 7

Aufgabe 7.1. Sei R ein reell abgeschlossener Körper, und seien $n, m, k \in \mathbb{N}^*$. Seien $A \subseteq R^n$ und $B \subseteq R^m$ semialgebraische Mengen. Zeigen Sie:

a) Sind $f\colon A \to B$ und $g\colon B \to R^k$ semialgebraische Funktionen, so auch $g \circ f\colon A \to R^k$.

b) Eine Abbildung $f\colon A \to B$ ist genau dann semialgebraisch, wenn für jede semialgebraische Funktion $g\colon B \to R$ die Komposition $g \circ f\colon A \to R$ semialgebraisch ist.

c) Seien $f_1, \ldots, f_m\colon A \to R$ Abbildungen. Die Abbildung $f = (f_1, \ldots, f_m)\colon A \to R^m$, $a \mapsto (f_1(a), \ldots, f_m(a))$ ist genau dann semialgebraisch, wenn alle f_j semialgebraisch sind.

d) Sei $f\colon A \to R$ semialgebraische Funktion, für die $f(a) \neq 0$ für alle $a \in A$ gilt. Dann ist auch $\frac{1}{f}\colon A \to R$, $a \mapsto \frac{1}{f(a)}$ semialgebraisch.

e) Sind $f, g\colon A \to R$ semialgebraische Funktionen, so auch $\sup(f, g)\colon A \to R$, $a \mapsto \sup\{f(a), g(a)\}$ und $\inf(f, g)\colon A \to R$, $a \mapsto \inf\{f(a), g(a)\}$.

f) Ist $f\colon A \to R^m$ eine semialgebraische Funktion, so ist $f^{-1}(B)$ semialgebraisch.

g) Ist $f\colon A \to B$ eine semialgebraische Bijektion, so ist auch die Umkehrabbildung $f^{-1}\colon B \to A$ semialgebraisch.

Aufgabe 7.2. Sei $S \subseteq R^n$ eine nichtleere semialgebraische Menge über einem reell abgeschlossener Körper R. Zeigen Sie:

a) Für alle $x \in R^n$ ist der *Abstand* zwischen x und S

$$\operatorname{dist}(x, S) := \inf\{\|x - y\| \mid y \in S\}$$

wohldefiniert.

b) Die Funktion $\operatorname{dist}_S\colon R^n \to R$, $x \mapsto \operatorname{dist}(x, S)$ ist stetig und semialgebraisch, sie verschwindet auf dem Abschluß $\overline{S}$ von S, ist aber überall sonst positiv.

Aufgabe 7.3. Sei R ein reell abgeschlossener Körper, und sei $n \in \mathbb{N}^*$. Zeigen Sie, dass die semialgebraischen Mengen

$$R^n,\ ]0,\infty[^n,\ ]0,1[^n \text{ und } B_n := \{x \in R^n \mid \|x\| < 1\}$$

alle zueinander semialgebraisch homöomorph sind.

Aufgabe 7.4. Sei $(K, \leq)$ ein angeordneter Körper, sei $n \in \mathbb{N}^*$, und sei $K[X_1, \ldots, X_n]$ der Polynomring in n Unbestimmten über K. Sei $a = (a_1, \ldots, a_n) \in K^n$ gegeben. Zeigen Sie, dass die Menge $P := P_a := \{f \in K[X_1, \ldots, X_n] \mid f(a) \geq 0\}$ folgende Eigenschaften besitzt:

a) $P + P \subseteq P$, $P \cdot P \subseteq P$, $K[X_1, \ldots, X_n]^2 \subseteq P$ und $-1 \notin P$;

b) $P \cup -P = K[X_1, \ldots, X_n]$ und $P \cap -P$ ist ein Primideal von $K[X_1, \ldots, X_n]$.

Sei nun $b \in K^n$ mit $b \neq a$. Betrachten Sie die Menge $T := P_a \cap P_b = \{f \in K[X_1, \ldots, X_n] \mid f(a) \geq 0,\ f(b) \geq 0\}$. Welche der oben genannten Eigenschaften sind auch für T erfüllt? Welche nicht?

Übungsblatt 8

Definition 7. Sei X eine Menge. Sei $\mathcal{U} \subseteq \mathcal{P}(X)$ eine Teilmenge der Potenzmenge von X. Man sagt, dass $\mathcal{U}$ die *endliche Durchschnittseigenschaft* hat, wenn jeder Durchschnitt endlich vieler Elemente von $\mathcal{U}$ nicht leer ist.

Ist X ein topologischer Raum, so heißt X

(i) *quasikompakt*, wenn jede Überdeckung von X durch offene Mengen eine endliche Teilüberdeckung besitzt;

(ii) *hausdorffsch*, wenn es zu je zwei verschiedenen Punkten $x, y \in X$ offene Mengen $U, V \subseteq X$ mit $x \in U$, $y \in V$ und $U \cap V = \emptyset$ gibt;

(iii) *kompakt*, wenn er quasikompakt und hausdorffsch ist.

Aufgabe 8.1. Sei X ein topologischer Raum. Zeigen Sie:

a) X ist genau dann quasikompakt, wenn jede nichtleere, aus abgeschlossenen Teilmengen von X bestehende Menge $\mathcal{U} \subseteq \mathcal{P}(X)$, die die endliche Durchschnittseigenschaft besitzt, einen nichtleeren Durchschnitt $\bigcap \mathcal{U} = \bigcap_{U \in \mathcal{U}} U$ hat.

b) Ist X quasikompakt, so auch jede abgeschlossene Teilmenge von X, wenn man sie als topologischen Raum, der mit der Spurtopologie versehen ist, betrachtet.

c) Ist X hausdorffsch, so ist jede kompakte Teilmenge von X abgeschlossen in X.

Aufgabe 8.2. (Satz von Tychonoff)
Ist $(X_i)_{i \in I}$ eine Familie quasikompakter topologischer Räume, so ist auch der mit der Produkttopologie versehene Raum $X = \prod_{i \in I} X_i$ quasikompakt.
(Anleitung: Sei $\mathcal{U} \subseteq \mathcal{P}(X)$ eine aus abgeschlossenen Teilmengen von X bestehende Menge mit der endlichen Durchschnittseigenschaft. Zeigen Sie, dass Sie $\mathcal{U}$ in $\mathcal{P}(X)$ als maximal bezüglich der endlichen Durchschnittseigenschaft annehmen können. Betrachten Sie nun zu jedem $i \in I$ die Menge $V_i := \bigcap_{U \in \mathcal{U}} \overline{\pi_i(U)}$, wobei π_i die Projektion von X auf die i-te Komponente X_i sei. Zeigen Sie, dass Sie (mit dem Auswahlaxiom) ein Element

$a = (a_i)_{i\in I} \in \prod_{i\in I} V_i$ wählen können. Erinnern Sie sich an die kanonische Basis der Produkttopologie und zeigen Sie dann, dass $a \in \overline{U}$ für jedes $U \in \mathcal{U}$ ist.)

Aufgabe 8.3. Sei A ein kommutativer Ring. Wir betrachten $\operatorname{Sper} A$ zusammen mit der spektralen Topologie. Zeigen Sie:

a) Für $P, Q \in \operatorname{Sper} A$ gilt $P \in \overline{\{Q\}}$ genau dann, wenn $Q \subseteq P$ ist.

b) $\operatorname{Sper} A$ ist im Allgemeinen nicht hausdorffsch.

c) Der Teilraum $\operatorname{Sper}^{\max}(A)$ der maximalen Positivbereiche von A ist kompakt.

Aufgabe 8.4. Sei A ein kommutativer Ring mit 1, und sei S eine multiplikatives System von A, d.h. S ist multiplikativ abgeschlossen und die 1 ist in S enthalten. Sei $S^{-1}A$ die Lokalisierung von A nach S. Seien $\operatorname{Sper} A$ und $\operatorname{Sper} S^{-1}A$ mit der spektralen Topologie versehen. Zeigen Sie:

a) Der Ringhomomorphismus $\iota\colon A \to S^{-1}A,\ a \mapsto \frac{a}{1}$, induziert eine stetige Abbildung $\iota^*\colon \operatorname{Sper} S^{-1}A \to \operatorname{Sper} A$.

b) $\operatorname{Sper} S^{-1}A$ ist homöomorph zum Teilraum $\{P \in \operatorname{Sper} A \mid \operatorname{supp}(P) \cap S = \emptyset\}$ von $\operatorname{Sper} A$.

Übungsblatt 9

Definition 8. Sei A ein kommutativer Ring, und sei $P \in \operatorname{Sper} A$. Ein Ideal I von A heißt

(i) *P-konvex*, wenn aus $a, b \in P$ und $a+b \in I$ stets $a \in I$ (und damit auch $b \in I$) folgt.

(ii) ein *P-Radikal*, wenn aus $a \in A$, $b \in P$ und $a^2 + b \in I$ folgt, dass a in I liegt.

Aufgabe 9.1. Sei A ein kommutativer Ring, und sei $P \in \operatorname{Sper} A$.

a) Zeigen Sie, dass $\operatorname{supp}(P)$ ein P-konvexes Ideal von A ist.

b) Seien I, J P-konvexe Ideale von A. Zeigen Sie, dass dann auch $I + J$ und $I \cap J$ P-konvexe Ideale von A sind.

c) Seien I, J P-konvexe Ideale von A. Ist dann auch stets IJ ein P-konvexes Ideal?

d) Sei I ein P-konvexes Ideal von A. Ist dann das Radikal $\sqrt{I}$ von I auch P-konvex?

e) Sei I ein P-konvexes Ideal mit $I \neq A$. Zeigen Sie, dass dann $\sqrt{I}$ ein Primideal ist.

f) Sei I ein Ideal von A. Zeigen Sie, dass I genau dann ein P-Radikal ist, wenn es P-konvex ist und $I = \sqrt{I}$ gilt.

g) Sei I ein Ideal von A mit $I \neq A$.
Zeigen Sie, dass I genau dann P-konvex ist, wenn $\overline{P} = \{a + I \mid a \in P\}$ ein Präpositivbereich auf A/I mit $\overline{P} \cup -\overline{P} = A/I$ und $\overline{P} \cap -\overline{P} = \{0\}$ ist.
Ist I ein P-konvexes Ideal, so definiert also $a + I \leq_{\overline{P}} b + I :\iff (b-a) + I \in \overline{P}$ eine lineare Ordnung auf A/I, die verträglich mit den Ringoperationen ist.
Ist I zusätzlich ein Primideal, so ist $\overline{P}$ ein Positivbereich mit $\operatorname{supp}(\overline{P}) = (0 + I)$. Insbesondere ist I dann reell.

Aufgabe 9.2. Sei A ein kommutativer Ring. Für $a \in A$ und $P \in \operatorname{Sper} A$ sei $a(P) := \alpha_P(a)$. Seien $P, Q \in \operatorname{Sper} A$. Wir bezeichnen mit $\langle P, Q\rangle$ das Ideal in A, das von allen $a \in A$ mit $a(P) \geq 0$ und $a(Q) \leq 0$ erzeugt wird. $\langle P, Q\rangle$ heißt das *Trennungsideal* oder *separierende Ideal* von P und Q.
Sei nun $a \in A$ mit $a \in P$, d.h. $a(P) \geq 0$. Zeigen Sie, dass genau dann $a \in \langle P, Q\rangle$ ist, wenn es ein $b \in A$ mit $a(P) \leq b(P)$ und $b(Q) \leq 0$ gibt.
(Anleitung: Zunächst einmal können Sie auch $a(Q) \geq 0$ annehmen. Ist $a \in \langle P, Q\rangle$, so ist $a = \sum_{i=1}^{n} c_i d_i$ für ein $n \in \mathbb{N}$ und gewisse $c_i, d_i \in A$ mit $c_i(P) \geq 0$ und $c_i(Q) \leq 0$. Ohne Beschränkung der Allgemeinheit dürfen Sie auch $d_i(P) \geq 0$ annehmen. Ändern Sie die d_i jetzt so ab, dass sie $d_i' \in A$ erhalten, für die $b := \sum_{i=1}^{n} c_i d_i'$ die gewünschten Eigenschaften besitzt.)

Definition 9. Sei A ein kommutativer Ring, und seien $P, Q \in \operatorname{Sper} A$. Wir sagen P ist eine *Spezialisierung* von Q, *Q spezialisiert nach P* oder Q ist eine *Generalisierung* von P, wenn $P \in \overline{\{Q\}}$ in $\operatorname{Sper} A$ (versehen mit der spektralen Topologie) gilt. Dafür schreiben wir $Q \rightsquigarrow P$. Nach Aufgabe 8.3 ist $Q \rightsquigarrow P$ äquivalent zu $Q \subseteq P$.

Aufgabe 9.3. Sei A ein kommutativer Ring. Seien $P, Q \in \operatorname{Sper} A$. Zeigen Sie:

a) $\operatorname{supp}(P) + \operatorname{supp}(Q) \subseteq \langle P, Q\rangle$.

b) $\langle P, Q\rangle$ ist sowohl P- als auch Q-konvex, und P und Q induzieren dieselbe lineare Ordnung (siehe Aufgabe 9.1 g)) auf $A/\langle P, Q\rangle$.

c) $\langle P, Q\rangle$ ist das kleinste Ideal von A, das die in b) gezeigten Eigenschaften besitzt.

d) Ist $\langle P, Q\rangle \neq A$, so ist $\sqrt{\langle P, Q\rangle}$ ein Primideal und der Träger (Support) der kleinsten gemeinsamen Spezialisierung von P und Q.

e) Es gilt $\langle P, Q\rangle \neq A$ genau dann, wenn P und Q eine gemeinsame Spezialisierung besitzen.

Übungsblatt 10

Aufgabe 10.1. (Satz von Dini)
Sei $X \neq \emptyset$ ein quasikompakter topologischer Raum. Es bezeichne $C(X, \mathbb{R})$ den Raum der stetigen reellwertigen Funktionen auf X, versehen mit der Maximumsnorm. Sei $f \in C(X, \mathbb{R})$, und sei $(g_n)_{n\in\mathbb{N}} \subseteq C(X, \mathbb{R})$ eine Folge, bei der für alle $x \in X$ die Folge $(g_n(x))_{n\in\mathbb{N}}$ monoton steigend ist und gegen $f(x)$ konvergiert. Zeigen Sie, dass dann $(g_n)_{n\in\mathbb{N}}$ in $C(X, \mathbb{R})$ gegen f konvergiert.

Aufgabe 10.2. (Satz von Stone-Weierstraß)
Sei $X \neq \emptyset$ ein kompakter topologischer Raum, und sei $C(X, \mathbb{R})$ die mit der Maximumsnorm versehene $\mathbb{R}$-Algebra der stetigen reellwertigen Funktionen auf X. Sei A eine $\mathbb{Q}$-Unteralgebra von $C(X, \mathbb{R})$, die die Punkte von X trennt, das heißt zu je zwei verschiedenen Punkten $x, y \in X$ existiert ein $f \in A$ mit $f(x) \neq f(y)$. Zeigen Sie, dass dann A dicht in $C(X, \mathbb{R})$ liegt, d.h. der Abschluß von A ist $C(X, \mathbb{R})$. Beweisen Sie dafür die folgenden Aussagen:

a) Der Abschluß von A ist eine $\mathbb{R}$-Unteralgebra von $C(X, \mathbb{R})$. Wir können nun also ohne Beschränkung der Allgemeinheit annehmen, dass A eine abgeschlossene $\mathbb{R}$-Unteralgebra von $C(X, \mathbb{R})$ ist.

b) Sei $f \in C(X, \mathbb{R})$ mit $0 \leq f \leq 1$ auf X, und sei $g_0 \in C(X, \mathbb{R})$ mit $0 \leq g_0 \leq \sqrt{f}$, wobei $\sqrt{f}$ die Funktion in $C(X, \mathbb{R})$ sei, die $x \in X$ auf $\sqrt{f(x)}$ abbildet. Dann konvergiert die durch $g_{n+1} := g_n + \frac{1}{2}(f - g_n^2)$ definierte Folge gegen $\sqrt{f}$ in $C(X, \mathbb{R})$.
(Hinweis: Verwenden Sie den Satz von Dini aus Aufgabe 10.1.)

c) Ist $f \in A$, so auch $|f| \colon X \to \mathbb{R}$, $x \mapsto |f(x)|$.

d) Sind $f, g \in A$, so auch die Abbildungen $\min\{f, g\} \colon X \to \mathbb{R}$, $x \mapsto \min\{f(x), g(x)\}$, und $\max\{f, g\} \colon X \to \mathbb{R}$, $x \mapsto \max\{f(x), g(x)\}$.

e) Zu je zwei verschiedenen Punkten $x, y \in X$ und beliebigen Zahlen $a, b \in \mathbb{R}$ gibt es ein $f \in A$ mit $f(x) = a$ und $g(y) = b$.

f) Ist $0 < \varepsilon \in \mathbb{R}$, $f \in C(X, \mathbb{R})$ und $x \in X$, so gibt es ein $g \in A$ mit $g(x) = f(x)$ und $g < f + \varepsilon$ auf X.
(Hinweis: Benutzen Sie die Kompaktheit von X, um g als das Minimum von endlich vielen geeigneten Funktionen zu wählen.)

g) Ist $0 < \varepsilon \in \mathbb{R}$ und $f \in C(X, \mathbb{R})$, so gibt es ein $g \in A$ mit $f - \varepsilon < g < f + \varepsilon$ auf X.
(Hinweis: Benutzen Sie die Kompaktheit von X, um g als das Maximum von endlich vielen geeigneten Funktionen zu wählen.)

Aufgabe 10.3. Zeigen Sie, dass für alle $x \in \mathbb{R}$

$$(1 - x^2)^3 \geq 0 \Rightarrow 1 - x^2 \geq 0$$

gilt, es aber dennoch keine Quadratsummen s, t in $\mathbb{R}[X]$ mit

$$1 - X^2 = s + t(1 - X^2)^3$$

gibt.

Übungsblatt 11

Definition 10. Sei L/K eine Körpererweiterung.

(i) Elemente $x_1, \ldots, x_n \in L$ heißen *algebraisch abhängig über* K, falls es ein von Null verschiedenes Polynom $p \in K[X_1, \ldots, X_n]$ mit $p(x_1, \ldots, x_n) = 0$ gibt. Ansonsten heißen $x_1, \ldots, x_n$ *algebraisch unabhängig über* K.

(ii) Eine Teilmenge $M \subseteq L$ heißt *algebraisch unabhängig über* K, falls je endlich viele paarweise verschiedene Elemente von M algebraisch unabhängig über K sind.

(iii) Eine Teilmenge $B \subseteq L$ heißt *Transzendenzbasis von* L/K, wenn sie algebraisch unabhängig über K ist und die Körpererweiterung $L/K(B)$ algebraisch ist.

Aufgabe 11.1. Sei L/K eine Körpererweiterung, und sei $B \subseteq L$ eine Teilmenge. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) B ist eine Transzendenzbasis von L/K.

(ii) B ist eine maximale über K algebraisch unabhängige Teilmenge von L.

(iii) B ist eine minimale Teilmenge von L derart, dass L algebraisch über $K(B)$ ist.

Aufgabe 11.2. Sei L/K eine Körpererweiterung. Zeigen Sie, dass eine Transzendenzbasis von L/K existiert.

Aufgabe 11.3. Sei L/K eine Körpererweiterung, und sei B eine endliche Transzendenzbasis von L/K. Zeigen Sie, dass jede weitere Transzendenzbasis von L/K die gleiche Mächtigkeit wie B hat.
(Hinweis: Wandeln Sie in geeigneter Weise den Beweis des Steinitzschen Austauschsatzes aus der Linearen Algebra ab.)

Definition 11. Sei L/K eine Körpererweiterung, und sei B eine Transzendenzbasis von L/K. Wir setzen

$$\operatorname{trdeg}(L/K) := \begin{cases} \#B, & \text{falls } \#B < \infty, \\ \infty & \text{sonst,} \end{cases}$$

und nennen dies den *Transzendenzgrad von* L/K.

Aufgabe 11.4. Sei L/K eine Körpererweiterung, und sei $L \supseteq E \supseteq K$ ein Zwischenkörper. Zeigen Sie, dass

$$\operatorname{trdeg}(L/K) = \operatorname{trdeg}(L/E) + \operatorname{trdeg}(E/K).$$

Übungsblatt 12

Aufgabe 12.1.

a) Sei K ein Körper, und sei $\mathfrak{p}$ ein Primideal von $K[X_1, \ldots, X_n]$. Bestimmen Sie den Transzendenzgrad von $L = \mathrm{Quot}(K[X_1, \ldots, X_n]/\mathfrak{p})$ über K für:

   (i) $\mathfrak{p} = (f)$ mit $f \in K[X_1, \ldots, X_n]$ irreduzibel.

   (ii) $\mathfrak{p} = (X_1 - a_1, \ldots, X_n - a_n)$ mit $a_1, \ldots, a_n \in K$.

b) Seien K ein Körper und $n \in \mathbb{N}$. Sei für $1 \leq k \leq n$

$$\sigma_k := \sum_{1 \leq i_1 < \cdots < i_k < n} X_{i_1} \cdots X_{i_k} \in K[X_1, \ldots, X_n]$$

   das k-te elementarsymmetrische Polynom. Bestimmen Sie den Transzendenzgrad von $L := K(\sigma_1, \ldots, \sigma_n)$ über K.

Aufgabe 12.2. Sei K ein algebraischer Zahlkörper. Zeigen Sie, dass dann jede Semiordnung von K schon eine Anordnung ist.

Aufgabe 12.3. Sei $A := \mathbb{R}[X, Y]$ der Polynomring in zwei Unbestimmten. Es bezeichne $<$ die lexikographische Ordnung auf $\mathbb{N} \times \mathbb{N}$, d.h. für alle $d = (d_1, d_2), e = (e_1, e_2) \in \mathbb{N}^2$ gilt genau dann $d < e$, wenn $d_1 < e_1$ oder $d_1 = e_1$ und $d_2 < e_2$. Dies ist eine lineare Ordnung auf $\mathbb{N}^2$, somit existiert zu jedem von Null verschiedenen Polynom

$$f(X, Y) = \sum_{d \in \mathbb{N}^2} a_d X^{d_1} Y^{d_2}$$

(mit $a_d \in \mathbb{R}$ und $a_d \neq 0$ nur für endliche viele $d \in \mathbb{N}^2$) ein kleinstes $d \in \mathbb{N}^2$ mit $a_d \neq 0$, welches wir mit $d(f)$ bezeichnen. Außerdem setzen wir $\mathrm{lc}(f) := a_{d(f)}$. Sei nun die Menge $S' \subseteq A \setminus \{0\}$ folgendermaßen definiert:

$$f \in S' :\Longleftrightarrow\ f \neq 0 \text{ und } \begin{cases} \mathrm{lc}(f) > 0 & \text{und} \quad d(f) \not\equiv (1,1) \bmod 2\mathbb{N}^2 \text{ oder} \\ \mathrm{lc}(f) < 0 & \text{und} \quad d(f) \equiv (1,1) \bmod 2\mathbb{N}^2. \end{cases}$$

Zeigen Sie, dass die Menge $S := S' \cup \{0\}$ eine Semiordnung von A mit $\mathrm{supp}(S) = \{0\}$ ist, aber keine Anordnung.

Aufgabe 12.4. Seien $f, h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$ lineare Polynome mit $W_{\mathbb{R}}(h_1, \ldots, h_s) =: W_{\mathbb{R}} \neq \emptyset$ und $f \geq 0$ auf $W_{\mathbb{R}}$. Zeigen Sie, dass dann nichtnegative Elemente $b_0, \ldots, b_s \in \mathbb{R}$ existieren, so dass

$$f = b_0 + b_1 h_1 + \cdots + b_s h_s.$$

(Anleitung: O.B.d.A. gilt $0 \in W_{\mathbb{R}}$. Homogenisieren Sie die Polynome $h_1, \ldots, h_s$ und f: Ist z.B. $f(X_1, \ldots, X_n) = l(X_1, \ldots, X_n) + \alpha$ mit l ein lineares homogenes Polynom (alle Monome haben Grad 1) und $\alpha \in \mathbb{R}$, so ist dessen Homogenisierung $F(X_0 X_1, \ldots, X_n) = l(X_1, \ldots, X_n) + \alpha X_0$. Analog erhält man auch aus $h_1, \ldots, h_s$ lineare homogene Polynome $H_1, \ldots, H_s$ in $n+1$ Unbestimmten. Zeigen Sie, dass $F \geq 0$ auf $W_{\mathbb{R}}(H_0, H_1, \ldots, H_s)$ mit $H_0 = X_0$. Fassen Sie nun die Linearformen $F, H_0, \ldots, H_s$ als Punkte im $\mathbb{R}^{n+1}$ auf.)

Literatur

[1] A.J. Engler, A. Prestel. *Valued Fields*. Springer Verlag, 2005.

[2] A. Prestel, C.N. Delzell. *Positive Polynomials*. Springer Verlag, 2001.