Seminar Auswahlaxiom A:
Das Auswahlaxiom und Wurzelfunktionen in Ringen

Fabrice Gärtner und Simon Müller

April 2020

1 Die Auswahlprinzipien nRR und AC'

Um uns auf die Hauptaussage dieser Präsentation vorzubereiten, wollen wir in diesem Kapitel die grundlegenden Begriffe einführen und versuchen intuitiv zu verstehen, wie diese mit dem Auswahlaxiom in Verbindung gebracht werden können. Wir werden uns hier ausschliesslich mit kommutativen Ringen beschäftigen und weil nullte oder erste Wurzeln nicht sehr interessant sind, wollen wir $n > 1$ annehmen.

1.1 nRR

Zuerst wollen wir verstehen, was es mit dieser kryptischen Abkürzung auf sich hat. Hinter nRR verbirgt sich nichts anderes als die Kurzform von: Existenz einer n-ten Wurzelfunktion (englisch: root) in einem Ring.

Definition 1.1. Wir definieren das Auswahlprinzip nRR:

In jedem Ring existiert eine n-te Wurzelfunktion.

Im Folgenden werden wir den Begriff der Wurzelfunktion noch etwas präzisieren und uns einige Gedanken machen, wie sie mit dem Auswahlaxiom zusammenhängt.
Sei nun also R ein kommutativer Ring und n eine natürliche Zahl. Um für diesen Ring zu definieren, was eine Wurzelfunktion ist, müssen wir erst die Menge der n-ten Potenzen definieren:

Definition 1.2. Menge der n-ten Potenzen:

$$R^{(n)} := \{x^n : x \in R\}$$

Die Definition ist durch die folgende Überlegung motiviert: wir wollen uns die Wurzelfunktion intuitiv als etwas Inverses zur Potenzierung vorstellen. Also macht es nur Sinn, die Wurzelfunktion auf Elementen von der Form x^n anzuwenden. Mit der obigen Definition haben wir uns also die Definitionsmenge einer Wurzelfunktion handlich bereitgelegt. Mit der Erkenntnis, dass $0 = 0^n \in R^{(n)}$ sehen wir auch, dass diese Menge für alle Ringe nichtleer ist und wir also auch wirklich etwas zu behandeln haben. Die formale Definition einer Wurzelfunktion ist nun:

Definition 1.3. Eine Funktion $f : R^{(n)} \mapsto R$ ist eine n-te Wurzelfunktion, falls für alle $y \in R^{(n)}$ gilt: $f(y)^n = y$.

Hier haben wir tatsächlich nur definiert, was wir uns vorher schon überlegt hatten. Nämlich soll die Wurzelfunktion durch die n-te Potenz wieder rückgängig gemacht werden. Mathematisch bedeutet dies, dass sie eine Rechtsinverse der n-ten Potenz ist. Welche Schwierigkeiten bei der Definition von Wurzelfunktionen auftreten können, überlegen wir uns am folgenden Beispiel.

Beispiel 1.4. Betrachten wir den Ring der ganzen Zahlen $R = \mathbb{Z}$ und $n = 2$. Wir erkennen schnell, dass nicht jedes Element überhaupt eine n-te Wurzel besitzt. Da wäre die Zahl 17. Man kann sich leicht davon überzeugen, dass es kein $z \in \mathbb{Z}$ gibt, sodass $z^2 = 17$. Deshalb haben wir vorher die Menge der n-ten Potenzen definiert und uns bei der Definition einer Wurzelfunktion auf diese beschränkt.
Eine weitere wichtige Erkenntnis aus diesem Beispiel ist, dass ein Element mehrere n-te Wurzeln haben kann. Wenn wir beispielsweise die Zahl 4 betrachten, dann ist offenbar sowohl $2^2 = 4$ als auch $(-2)^2 = 4$. Allgemein gilt, dass für alle $0 \neq z \in \mathbb{Z}^{(2)}$ jeweils genau eine positive und eine negative Wurzel existiert.
Wollen wir auf $\mathbb{Z}$ eine Wurzelfunktion definieren, müssen wir uns also eine der beiden Wurzeln aussuchen. Eine Funktion ist ja unter anderem dadurch definiert, dass wir für ein Element nicht mehrere Bilder haben dürfen.
In diesem Beispiel kommen wir noch um den Einsatz des Auswahlaxioms herum. Mit der bekannten Ordnung auf $\mathbb{Z}$ können wir uns die Wurzeln mit einer Regel aussuchen. Normalerweise wählt man die positive.

In allgemeinen Ringen können wir allerdings nicht immer eine solche Regel aufstellen. Wir können auch nicht hoffen, dass wir nur aus endlich vielen Wurzeln auswählen müssen. An diesem Punkt müssen wir das Auswahlaxiom ins Spiel bringen, um Wurzelfunktionen definieren zu können.

1.2 AC'

Als Zweites wollen wir ein Auswahlprinzip vorstellen, welches dem Auswahlaxiom sehr ähnlich ist. Dafür rufen wir uns erst das klassische Auswahlaxiom in Erinnerung.

Definition 1.5. Wir definieren das Auswahlprinzip AC:

Für jede Familie $\mathscr{F}$ von nichtleeren Mengen existiert eine Auswahlfunktion f, die aus jeder Menge ein Element aussucht. Formaler bedeutet dies, dass

$$\text{für jedes } Y \in \mathscr{F} : f(Y) \in Y.$$

Wir bemerken, dass unsere Auswahlfunktion aus jeder Menge nur genau ein Element auswählt. Im Folgenden stellen wir uns die Frage, ob es denn auch möglich ist, mehr als nur ein Element auszuwählen und ob dies äquivalent zum klassischen Auswahlaxiom ist. Wenn wir für eine Menge mehr als ein Element auswählen wollen, können wir uns das vorstellen, als würden wir eine Teilmenge auswählen. Weil die Wahl der ganzen Menge etwas uninspirierend ist, beschränken wir uns, wann immer möglich, auf echte Teilmengen. Natürlich geht das nur, wenn die Menge mehr als ein Element hat. Wir halten das in der folgenden Definition fest.

Definition 1.6. Wir definieren das Auswahlprinzip AC':

Für jede Familie $\mathscr{F}$ von nichtleeren Mengen existiert eine Funktion, die aus jeder Menge ein Singleton oder eine echte Teilmenge auswählt.

etwas formaler:

Es existiert eine Funktion $f : \mathscr{F} \mapsto \bigcup_{Y \in \mathscr{F}} \mathscr{P}(Y) \setminus \{\emptyset\}$ mit der Eigenschaft, dass für $Y \in \mathscr{F}$ gilt $g(Y) \subsetneq Y$, ausser wenn $|Y| = 1$, dann gilt $g(Y) = Y$.

Im nächsten Kapitel werden wir zu diesen Definitionen auch mathematisch interessante und wertvolle Aussagen anschauen und die eingeführten Auswahlprinzipien mit dem Auswahlaxiom verbinden.

2 Äquivalente Aussagen zum Auswahlaxiom

2.1 Einführende Überlegungen

In diesem Kapitel wollen wir unter anderem beweisen, dass nRR und AC' äquivalent sind zum klassischen Auswahlaxiom. Auf den ersten Blick mag es plausibel erscheinen, dass mit dem Auswahlaxiom, welches für beliebige Kollektionen von Mengen gilt, Aussagen über Ringe gezeigt werden können. Andererseits ist es umso faszinierender, dass mit einer Wurzelfunktion auf einem Ring (einer Menge mit relativ viel Struktur) eine Auswahlfunktion für beliebige Mengensysteme konstruiert werden kann.

2.2 Äquivalenz der Auswahlprinzipien

Wir kommen nun zum Herzstück von dieser Präsentation:

Theorem 2.1. Die folgenden Aussagen sind äquivalent:

i) AC

ii) nRR gilt für alle $n > 1$

iii) $\exists n \in \mathbb{N}_{>1}$: nRR

iv) AC'

Beweis. i)⇒ ii): Idee: Für ein fixes n und einen Ring R betrachten wir für jedes Element von R die (womöglich leere) Menge von n-ten Wurzeln. Auf diese Kollektion von Mengen wenden wir das Auswahlaxiom an und können damit jedem Element des Ringes eine eindeutige n-te Wurzel zuordnen (falls so eine existiert). Formal: Sei R ein Ring und $n \in \mathbb{N}$. Definiere wie im ersten Kapitel

$$R^{(n)} := \{x^n : x \in R\}.$$

Betrachte ferner folgende Äquivalenzrelation auf R:

$$x \sim \tilde{x} \Leftrightarrow x^n = \tilde{x}^n.$$

Somit sind zwei Elemente aus R äquivalent genau dann, wenn sie n-te Wurzeln desselben Ringelementes sind. Wir wenden nun das Auswahlaxiom auf die Menge der Äquivalenzklassen an:

$$\mathscr{F} := R/\sim = \{[x] : x \in R\},$$

wobei $[x]$ die Äquivalenzklasse von x bezeichne. $\mathscr{F}$ partitioniert R in nichtleere, paarweise disjunkte Mengen. Somit existiert wegen AC eine Auswahlfunktion f auf $\mathscr{F}$. Wir definieren

$$\begin{aligned} \sqrt[n]{\cdot} : R^{(n)} &\longrightarrow R \\ y &\longmapsto f([x]), \end{aligned}$$

wobei $[x]$ so gewählt ist, dass $[x] = \{\tilde{x} \in R : \tilde{x}^n = y\}$. Dies zeigt, dass $\sqrt[n]{\cdot}$ tatsächlich eine n-te Wurzelfunktion von R ist.

ii)⇒ iii): trivial

iii)⇒ iv): Nun wissen wir, dass jeder Ring eine n-te Wurzelfunktion besitzt

für ein $n \in \mathbb{N}$. Für eine beliebige Kollektion $\mathscr{F}$ von Mengen wollen wir einen geeigneten Polynomring konstruieren, sodass uns eine n-te Wurzelfunktion gerade eine Auswahlfunktion im Sinne von iv) ergibt.
Sei nun Λ eine beliebige Indexmenge und sei $\mathscr{F} = \{Y_\iota : \iota \in \Lambda\}$ eine beliebige Kollektion von paarweise disjunkten, nicht-leeren Mengen. Sei weiter $\mathscr{A} = \bigcup \mathscr{F}$ die Vereinigung über alle Mengen von $\mathscr{F}$, d.h. $\mathscr{A}$ enthält alle Elemente der Mengen aus $\mathscr{F}$. Betrachte nun $\mathbb{Z}[\mathscr{A} \cup \mathscr{F}]$ (Polynomring über $\mathbb{Z}$ mit den Mengen aus $\mathscr{F}$ und den Elementen aus $\mathscr{A}$ als Unbestimmte).
Der Trick besteht nun darin, ein geeignetes Ideal I in diesem Ring zu wählen und eine Wurzelfunktion auf dem Quotientenring zu betrachten. Unser Ziel ist es dabei, dass im Quotientenring die Elemente einer Menge Y aus der Kollektion $\mathscr{F}$ gerade n-te Wurzeln von Y sind. Sei also I das Ideal erzeugt von Elementen der Gestalt

$$s \cdot t \qquad \forall s, t \in \mathscr{A} \cup \mathscr{F} \text{ mit } s \neq t \tag{1}$$

$$x^n - Y \qquad \forall x \in \mathscr{A} \text{ und } Y \in \mathscr{F} \text{ s.d. } x \in Y \tag{2}$$

Die erste Relation wird später eine nützliche Darstellung des Quotientenringes als freier $\mathbb{Z}$-Modul erlauben und die zweite Relation impliziert, dass im Quotientenring die Elemente jeder Menge Y aus $\mathscr{F}$ gerade n-te Wurzeln von Y sind.
Nun gilt zum Beispiel wegen (1) und (2) für ein Y aus $\mathscr{F}$ und $x \in Y$ gerade

$$Y^2 \overset{(2)}{\equiv} x^n \cdot Y \equiv x^{n-1} \cdot (x \cdot Y) \overset{(1)}{\equiv} 0 \bmod I. \tag{3}$$

Schliesslich definieren wir

$$R := \mathbb{Z}[\mathscr{A} \cup \mathscr{F}] \,/\, I.$$

Sei ferner für jedes $k \in \mathbb{N}$

$$\mathscr{A}^{(k)} := \{x^k : x \in \mathscr{A}\}.$$

R besitzt als Quotient eines Polynomringes über $\mathbb{Z}$ eine natürliche $\mathbb{Z}$-Modul Struktur. Wegen (1) besteht jedes Monom (bzw. dessen Äquivalenzklasse) in R aus nur einer Unbestimmten. Zudem kann ein Y aus $\mathscr{F}$ wegen (3) in keiner höheren Potenz als 1 auftreten. Ferner garantiert (2), dass kein $x \in \mathscr{A}$ in einer höheren Potenz als $n-1$ vorkommt. Diese Bemerkungen implizieren, dass R ein freier $\mathbb{Z}$-Modul über $\{1\} \cup \mathscr{A}^{(1)} \cup \mathscr{A}^{(2)} \cup \ldots \cup \mathscr{A}^{(n-1)} \cup \mathscr{F}$ ist. Somit haben wir folgenden $\mathbb{Z}$-Modul Isomorphismus:

$$R = \mathbb{Z}1 \oplus A^{(1)} \oplus A^{(2)} \oplus \ldots \oplus A^{(n-1)} \oplus F,$$

wobei $A^{(k)}$ und F die freien $\mathbb{Z}$-Moduln über $\mathscr{A}^{(k)}$ bzw. $\mathscr{F}$ sind. Es kann auch überprüft werden, dass es sich hier um einen Ringisomorphismus handelt. Sei nun $\pi_{\cup Y}$ für $Y \in \mathscr{A}$ die kanonische Projektion

$$\pi_{\cup Y} : R \longrightarrow \bigoplus_{x \in Y} \mathbb{Z}x \subset A^{(1)}$$

und sei π_1 die Projektion

$$\pi_1 : R \longrightarrow \mathbb{Z}1.$$

Es kann leicht überprüft werden, dass π_1 ein Ringmorphismus ist (unter der Identifikation $\mathbb{Z}1 = \mathbb{Z}$). Im Folgenden identifizieren wir Elemente von $\mathscr{F}$ und $\bigcup \mathscr{F}$ mit den entsprechenden Elementen aus F und $A^{(1)}$.
Nun haben wir unseren gewünschten Ring konstruiert und wir können auf R das Auswahlprinzip nRR anwenden: Sei

$$\sqrt[n]{\cdot} : R^{(n)} \longrightarrow R$$

eine n-te Wurzelfunktion auf R. Wir wollen ausgehend von dieser Wurzelfunktion für jede Menge Y aus $\mathscr{F}$ eine Teilmenge wie in iv) finden, indem wir Wurzeln von Y in R betrachten. Sei also $r = \sqrt[n]{Y}$ für ein Y aus $\mathscr{F}$ (so ein r existiert, weil nach Annahme eine n-te Wurzelfunktion auf $R^{(n)}$ existiert und da $x^n = Y \ \forall x \in Y$, folgt $Y \in R^{(n)}$). Es gilt

$$0 = \pi_1(Y) = \pi_1(r^n) = \pi_1(r)^n.$$

Da $\pi_1(r) \in \mathbb{Z}$, folgt aus obiger Gleichung $\pi_1(r) = 0$. Sei $s := \pi_{\cup Y}(r)$ und $t := r - s$. Dann folgt mit $\pi_1(r) = 0$

$$s \in \bigoplus_{x \in Y} \mathbb{Z}x \quad \text{und} \quad t \in \bigoplus_{x \in \mathscr{A} \setminus Y} \mathbb{Z}x \oplus \bigoplus_{k=2}^{n-1} A^{(k)} \oplus F.$$

Betrachte nun $Y = r^n = (s+t)^n$. Wegen (1) verschwinden alle gemischten Terme beim Ausmultiplizieren von $(s+t)^n$ und wir erhalten $Y = s^n + t^n$. Der Term t^n verschwindet ebenfalls (das kann gezeigt werden, indem man t als Summe von (Potenzen von) Elementen aus $\mathscr{A} \cup \mathscr{F} \setminus \bigcup Y$ ausschreibt und ausmultipliziert. Mit (1) und (2) kann man zeigen, dass $t^n = 0$ gilt). Da $s \in \bigoplus_{x \in Y} \mathbb{Z}x$, kann s auch als Summe geschrieben werden:

$$s = \sum_{i=1}^{m} \alpha_i x_i,$$

für $\alpha_i \in \mathbb{Z}$ und $x_i \in Y$ (Beachte; s lässt sich als *endliche* Summe darstellen, da s Element eines freien Moduls und deshalb eine *endliche* Linearkombination der Erzeuger ist). Unter Verwendung von (1) erhalten wir

$$Y = s^n = \left(\sum_{i=1}^{m} \alpha_i x_i \right)^n = \sum_{i=1}^{m} \alpha_i^n (x_i)^n = \sum_{i=1}^{m} \alpha_i^n Y$$

und somit

$$\sum_{i=1}^{m} \alpha_i^n = 1.$$

Jetzt können wir eine Abbildung $g: \mathscr{F} \longrightarrow \bigcup_{Y \in \mathscr{F}} \mathscr{P}(Y)$ definieren, welche die Bedingungen von AC' erfüllt. Wir unterscheiden hierzu zwei Fälle:
Fall 1: n ist gerade: Dann gilt $\alpha_i^n \geq 0$ und da wir $\alpha_i \in \mathbb{Z}$ haben, folgt $m = 1$ und $\alpha_1 = \pm 1$. Wir setzen $g(Y) := \{x_1\}$.
Fall 2: n ist ungerade: Dann gilt entweder $m = 1$ und $\alpha_1 = 1$ oder es existieren Indices $i \neq j$ so dass $\alpha_i > 0$ und $\alpha_j < 0$. Wir definieren $g(Y) := \{x_i : \alpha_i > 0\}$. Bemerke, dass dies $\emptyset \subsetneq g(Y) \subsetneq Y$ impliziert (falls $|Y| > 1$). Ausserdem ist $g(Y)$ endlich, da m endlich ist.
Somit erfüllt $g(Y)$ sowohl im Fall 1 als auch im Fall 2 die gewünschten Anforderungen und g ist eine Auswahlfunktion wie in iv).

iv)⇒ i): Idee: Die Idee in diesem Beweisschritt besteht darin, AC' iteriert auf ein Y aus $\mathscr{F}$ anzuwenden. Konkret wählen wir zuerst mit AC' eine endliche und echte Teilmenge Y' von Y aus. Besteht diese Teilmenge aus nur einem Element, so sind wir fertig. Andernfalls wenden wir AC' auf Y' an und erhalten erneut eine endliche Teilmenge. Diesen Prozess können wir nun iterieren, bis wir schliesslich eine einelementige Teilmenge von Y erhalten. Wir wissen, dass dieser Prozess nach endlich vielen Schritten endet, da Y' endlich ist und wir gemäss AC' bei jedem Schritt eine strikt kleinere Menge wählen können. Kommen wir zum formalen Beweis:

Sei $\mathscr{F}$ eine Kollektion von nichtleeren Mengen. Sei $\mathscr{F}'$ die Kollektion aller Teilmengen (ausser der leeren Menge) von Mengen aus $\mathscr{F}$, das heisst $\mathscr{F}' := \bigcup_{Y \in \mathscr{F}} \mathscr{P}(Y) \setminus \emptyset$. Nach AC' existiert eine Auswahlfunktion

$$g: \mathscr{F}' \to \bigcup_{A \in \mathscr{F}'} \mathscr{P}(A) \setminus \emptyset = \mathscr{F}'.$$

Bemerke hierzu, dass für ein A aus $\mathscr{F}'$ nach Konstruktion auch alle Teilmengen (ausser $\emptyset$) zu $\mathscr{F}'$ gehören, denn A ist eine Teilmengen von einem Y aus $\mathscr{F}$. Da aber alle Teilmengen von Y zu $\mathscr{F}'$ gehören, sind folglich auch alle Teilmengen von A Bestandteil von $\mathscr{F}'$.
Eine Auswahlfunktion auf $\mathscr{F}'$ anstatt auf $\mathscr{F}$ zu betrachten erlaubt uns wie in der Idee erläutert, immer kleinere Teilmengen ausgehend von einem Y aus $\mathscr{F}$ zu wählen. Würden wir g bloss auf $\mathscr{F}$ betrachten, könnte es vorkommen, dass $g(Y)$ nicht in der Kollektion $\mathscr{F}$ enthalten ist und somit wäre es nicht möglich, mit g eine echte Teilmenge von $g(Y)$ auszuwählen. Gehen wir zurück zum Beweis:

Für alle Y aus $\mathscr{F}$ ist $\bigcap_{n\in\mathbb{N}} g^n(Y)$ ein Singleton, da $g(Y)$ endlich ist und iteriertes Anwenden von g immer kleinere (nichtleere) Mengen liefert. Zudem gilt auch $\bigcap_{n\in\mathbb{N}} g^n(Y) \in Y$, da jede Menge im Schnitt in Y enthalten ist. Somit definiert

$$\begin{aligned} f : \mathscr{F} &\longrightarrow \bigcup \mathscr{F} \\ Y &\longmapsto \bigcap_{n\in\mathbb{N}} g^n(Y) \end{aligned}$$

eine Auswahlfunktion wie in AC. □

3 Wurzelfunktionen in Integritätsbereichen und Körpern

In diesem Abschnitt wollen wir uns weiterführende Gedanken zu Wurzelfunktionen in Integritätsbereichen (englisch: integral domains) und Körpern (englisch: fields) machen. Grundlegende Kenntnis dieser algebraischen Strukturen wird hier vorausgesetzt.
Einer der Gründe, wieso uns diese interessieren ist, dass im Beweis der Äquivalenz von nRR und AC ein Ring vorkommt, der Nullteiler hat. Will man Nullteiler vermeiden, kommt man unweigerlich auf die Frage ob analoge Aussagen auf Integritätsbereichen und Körpern gelten. Wir definieren die Existenz einer Wurzelfunktion analog zu der in Ringen. Für die Abkürzung verwenden wir die Kurzformen der englischen Begriffe.

Definition 3.1. Wir definieren das Auswahlprinzip nRF:

In jedem Körper existiert eine n-te Wurzelfunktion.

Definition 3.2. Analog definieren wir das Auswahlprinzip nRID:

In jedem Integritätsbereich existiert eine n-te Wurzelfunktion.

Da die Einschränkung von Ringen auf Körper und Integritätsbereiche eine doch recht starke ist, erwarten wir nicht, dass nRF oder nRID zum klassischen Auswahlaxiom äquivalent sind. Wir definieren deshalb ein schwächeres Auswahlprinzip, von dem wir dann zeigen, dass es die beiden impliziert.

Definition 3.3. Wir definieren das Auswahlprinzip C_n:

Für jede Familie von n-elementigen Mengen existiert eine Auswahlfunktion.

Für den Beweis der nächsten Proposition wird sich dieses Lemma, das wir hier ohne Beweis angeben, als nützlich erweisen.

Lemma 3.4. Sind m und n positive natürliche Zahlen und gilt $m \mid n$, dann gilt: $C_n \implies C_m$.

Proposition 3.5.

$$C_n \implies nRF$$

Beweis. Sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Wir definieren analog zu Ringen die Menge der n-ten Potenzen in $\mathbb{K}$.

$$\mathbb{K}^{(n)} := \{x^n : x \in \mathbb{K}\}$$

Wir erinnern uns an die Tatsache, dass für jedes $y \in \mathbb{K}$, das Polynom

$$X^n - y$$

höchstens n Nullstellen in $\mathbb{K}$ hat. Genauer gesagt gilt für alle $y \in \mathbb{K}^{(n)}$ mit $y \neq 0$, dass die Kardinalität der Menge

$$W_y := \{x \in \mathbb{K} : x^n = y\}$$

genau die Anzahl n-ter Einheitswurzeln in $\mathbb{K}$ ist. Schreiben wir $n = p^r \cdot k$, wobei p die Charakteristik des Körpers ist und p^r die höchste Potenz von p, die n teilt, dann ist die Anzahl n-ter Einheitswurzeln in einem Zerfällungskörper von $\mathbb{K}$ genau k. Insbesondere ist n teilbar durch k. Aus dem vorangegangenen Lemma folgt $C_n \implies C_k$.
Weiter ist klar, dass die n-ten Einheitswurzeln in $\mathbb{K}$ eine Untergruppe der n-ten Einheitswurzeln in einem beliebigen Zerfällungskörper sind. Daraus folgt mit Lagranges Theorem, dass diese Zahl n teilt und damit auch gilt:

$$|W_y| \mid n$$

Wir definieren nun

$$\mathscr{F} := \{W_y \subseteq \mathbb{K} : y \in \mathbb{K}^{(n)} \wedge y \neq 0\}$$

und wenden C_k darauf an um eine n-te Wurzelfunktion auf $\mathscr{F} \setminus \{0\}$ zu erhalten. Wählen wir nun 0 als n-te Wurzel von 0 erhalten wir eine n-te Wurzelfunktion auf ganz $\mathbb{K}^{(n)}$. □

Proposition 3.6.

$$nRF \iff nRID$$

Für den Beweis brauchen wir noch die folgenden Definitionen.

Definition 3.7. Sei S eine beliebige Menge. Eine *zyklische Ordnung* auf S ist eine Teilmenge $C \subseteq S \times S \times S$ mit den folgenden Eigenschaften:

1. Zyklisch: $(x,y,z) \in C \Rightarrow (y,z,x) \in C$
2. Asymmetrie: $(x,y,z) \in C \Rightarrow (z,y,x,) \notin C$
3. Transitivität: $(x,y,z) \in C \wedge (x,z,w) \in C \Rightarrow (x,y,w) \in C$
4. Totalität: Wenn x,y,z paarweise verschieden sind, dann gilt: $(x,y,z) \in C \vee (z,y,x) \in C$

Um die Notation $(x,y,z) \in C$ etwas abzukürzen, werden wir stattdessen $[x,y,z]$ schreiben. Wir stellen fest, dass für $|S| \leq 2$ die leere Menge $\emptyset$ eine zyklische Ordnung auf S ist.

Definition 3.8. Sei S eine zyklisch geordnete Menge und $s \in S$. Der *unmittelbare Nachfolger* von s ist das eindeutige Element s_+, für welches kein $t \in S$ existiert mit $[s,t,s_+]$

Unmittelbare Nachfolger existieren zwar nicht immer, aber darauf gehen wir nicht näher ein, weil wir zyklische Ordnungen hier nur auf endlichen Mengen verwenden und daher keine Probleme haben werden.

Beweis. " $\Leftarrow$ " : Da jeder Körper auch ein Integritätsbereich ist, ist diese Implikation trivial.
" $\Rightarrow$ " : Idee: Zu einem Integritätsbereich betrachten wir dessen Quotientenkörper. Darauf haben wir nach Annahme eine Wurzelfunktion. Diese modifizieren wir dann, in dem wir für die Elemente von R die Wurzelfunktion des Quotientenkörpers anwenden und diese Wurzel mit Hilfe des Konzepts von Nachfolgern in zyklischen Ordnungen in den Ring hinein manövrieren.
Formal: Sei R ein Integritätsbereich. Betrachte $\mathbb{K} := Quot(R) \supseteq R$, der Quotientenkörper von R (im englischen auch field of fractions genannt und mit Frac(R) bezeichnet). Sei $y \neq 0$ ein Element von $R^{(n)}$. Definiere wieder wie im ersten Beweis $W_y := \{x \in \mathbb{K} : x^n = y\}$. Wir bemerken, dass $k := |W_y|$ n teilt und unabhängig von y ist. Da für alle $y \in \mathbb{K}^{(n)}$ die Menge $\{\frac{x'}{x} : x,x' \in W_y\}$ eine zyklische Gruppe von Einheitswurzeln der Ordnung k und unabhängig von y ist, existiert ein primitive Einheitswurzel ζ.
Dieses ζ induziert nun eine zyklische Ordnung auf W_y wie folgt. Für $n = 2$ ist die zyklische Ordnung die leere Menge. Andernfalls ist für jedes $x \in W_y$ der unmittelbare Nachfolger gegeben durch ζx. Dies bedeutet, wir haben für

alle $x \in W_y$ dass $[x, x', x'']$ genau dann, wenn ganze Zahlen $0 < \alpha < \beta < k$ existieren, sodass $x' = \zeta^\alpha x$ und $x'' = \zeta^\beta x$.
Nach Annahme gibt es eine n-te Wurzelfunktion auf $\mathbb{K}^{(n)}$. Für ein $y \in R^{(n)}$ können wir nun nutzen, dass y auch in $\mathbb{K}^{(n)}$ ist. Wir betrachten dazu $\sqrt[n]{y}$, wobei die Wurzelfunktion diejenige des Körpers ist und die n-te Wurzel zwar sicher in $\mathbb{K}$ ist, aber nicht unbedingt in R sein muss. Die Wurzelfunktion auf R nimmt nun die Wurzel, die man mit der Funktion im Körper erhält, und wählt den ersten Nachfolger, der in R liegt.
Damit haben wir auch eine n-te Wurzelfunktion im Integritätsbereich definiert. □

Somit haben wir gezeigt, dass die Existenz von Wurzelfunktionen in Körpern äquivalent ist zu der in Integralbereichen. Mit der ersten Proposition und dieser Äquivalenz folgt nun auch direkt, dass $C_n \Rightarrow nRID$.