Einführung in die Algebra

Maxim Smirnov

Erstellt in Kollaboration mit Felix Geißler

Draft 19. Juli 2018

Inhaltsverzeichnis

Einführung

Dieses Script ersetzt nicht die Vorlesungen, da der Inhalt der Vorlesungen sich etwas unterscheiden kann. Manche Sachen (insbesondere Beispiele) werden in der Vorlesung ausführlicher behandelt als im Script und umgekehrt. Also er ist eher als ein "Roadmap" zu betrachten.

Jede Vorlesung bekommt im Script einen eigenen Abschnitt. Die kurze Wiederholung, die am Anfang jeder Vorlesung stattfindet, wird im Script weggelassen. Alle Definitionen, Sätze usw. werden innerhalb des Abschnittes nummeriert.

Es wird mit Nachdruck empfohlen zusätzlich zur Vorlesung Fachbücher zu benutzen. Als deutschsprachige Literatur werden die Bücher [B] und [KM] (insbesondere für Lehramtsstudierende) empfohlen. Als englischsprachige Literatur werden die Bücher [L] und [Sh]. Das letztere Buch gibt Ausblicke in fortgeschrittene Themenbereiche. Alle vier Bücher kann man über Uni Augsburg herunterladen. Hier sind die Links: Bosch, Karpfinger–Meyberg, Lang, Shafarevich.

Struktur: Die ersten drei Vorlesungen dienen als Schnupper-/Wiederholungsvorlesungen. In der ersten Vorlesung werden die komplexe Zahlen und der Begriff des Körpers eingeführt. In der zweiten Vorlesung fassen wir die benötigten Kenntnisse aus der linearen Algebra zusammen. In der dritten Vorlesung werden Matrizen und Operationen mit Matrizen eingeführt.

Vorlesungen 4 bis 8 sind der Einführung in die Gruppentheorie gewidmet. Insbesondere werden die Begriffe von Gruppe, Gruppenhomomorphismus, Gruppenwirkung, Normalteiler, Faktorgruppe eingeführt und mit vielen Beispielen illustriert.

Literatur

[B] S. Bosch. *Algebra.* Springer–Verlag Berlin Heidelberg 2009.

[KM] Ch. Karpfinger, K. Meyberg. *Algebra.* Spektrum Akademischer Verlag 2010.

[L] S. Lang. *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer–Verlag, New York, 2002. xvi+914.

[Sh] I.R. Shafarevich. *Basic notions of algebra.* Springer–Verlag Berlin Heidelberg 2005.

1 11.04.18 — Zahlensysteme

Aus der Schule kennt man folgende Zahlentypen:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Heute werden wir noch ein paar weitere Zahlensysteme (oder Arten von Zahlen) einführen, die wir später oft benutzen und verallgemeinern werden.

1.1 Komplexe Zahlen

Definition 1.1. Eine komplexe Zahl ist ein Ausdruck der Form

$$a + b\,i \tag{1.1}$$

mit $a, b \in \mathbb{R}$. Gegeben zwei komplexe Zahlen $a + bi$ und $c + di$, definiert man deren Summe als

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

und deren Produkt als

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \tag{1.2}$$

Die Menge aller komplexen Zahlen bezeichnet man mit $\mathbb{C}$.

Jede reelle Zahl $a \in \mathbb{R}$ kann man als komplexe betrachten, indem man (1.1) mit $b = 0$ verwendet. Dadurch erhalten wir eine Mengeninklusion

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

die mit Addition und Multiplikation kompatibel ist. Die Einheit $1 \in \mathbb{R}$ ist auch eine Einheit in $\mathbb{C}$, d.h. für jede $z = a + bi$ gilt $1 \cdot z = z$.

Nach Formel (1.2) gilt

$$i \cdot i = -1, \tag{1.3}$$

und man nennt die komplexe Zahl i imaginäre Einheit.

Für eine komplexe Zahl

$$z = a + bi$$

definiert man die komplex Konjugierte als

$$\bar{z} = a - bi,$$

und deren Betrag als

$$|z| = \sqrt{a^2 + b^2},$$

wobei die nicht negative Wurzel gemeint ist.

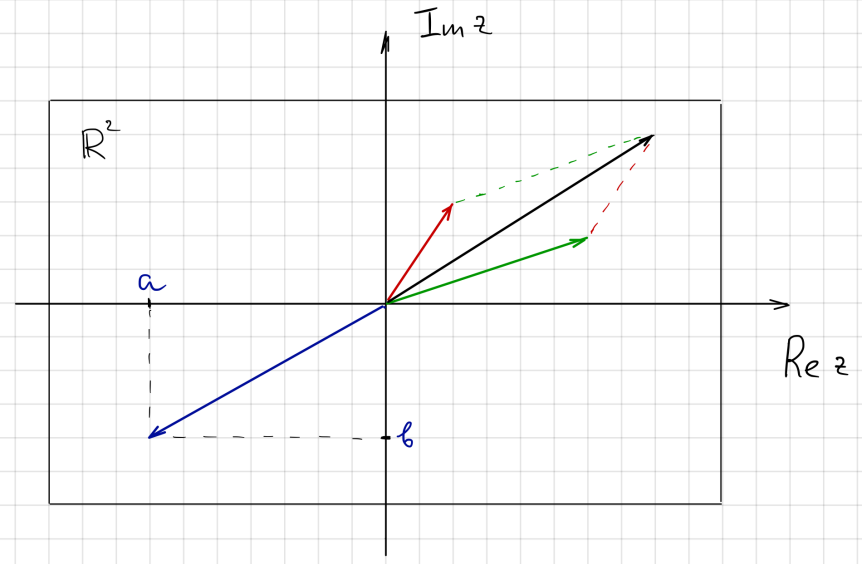
Man folgert aus (1.2), dass jede komplexe Zahl $z = a + bi \neq 0$ eine Inverse hat, die durch die Formel

$$\frac{1}{z} = \frac{a - ib}{a^2 + b^2} = \frac{\bar{z}}{|z|^2} \tag{1.4}$$

gegeben ist.

1.1.1 Geometrische Darstellung

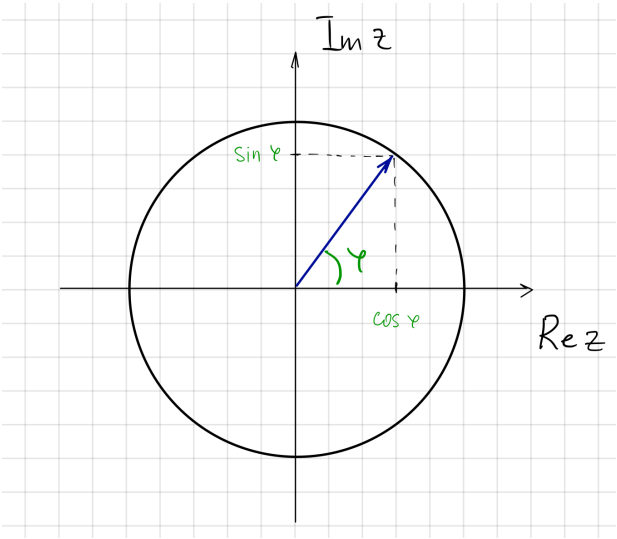
Man identifiziert die Menge $\mathbb{C}$ der komplexen Zahlen mit der reellen Ebene $\mathbb{R}^2$, d.h. eine komplexe Zahl $a + bi$ entspricht dem Punkt $(a, b) \in \mathbb{R}^2$.



Mit dieser Identifikation entspricht die Addition von komplexen Zahlen der Summe von Vektoren in in der Ebene $\mathbb{R}^2$. Die komplexe Konjugation entspricht der Spiegelung an der reellen Achse. Der Betrag $|z|$ ist die Länge des ensprechenden Vektors in $\mathbb{R}^2$.

1.1.2 Euler's Formel

Eine besondere Rolle spielen die komplexen Zahlen mit Betrag 1, d.h. die komplexe Zahlen, die auf dem Einheitskreis liegen.



So eine Zahl kann man schreiben als

$$z = \cos\varphi + i\sin\varphi.$$

Für jedes $\varphi \in \mathbb{R}$ definieren wir

$$e^{i\varphi} := \cos\varphi + i\sin\varphi. \tag{1.5}$$

Der Ausdruck (1.5) verhält sich ähnlich zu der Exponentialfunktion, d.h. die Rechenregel

$$e^{i(a+b)} = e^{ia}e^{ib} \tag{1.6}$$

gilt. Man kann (1.6) aus Additionstheoreme für Sinus- und Kosinusfunktionen leicht folgern (Übung). Es gibt aber auch andere Beweise (z.B. durch die Potenzreihenentwicklung).

1.1.3 Wurzeln

Aus der Schule ist bekannt, dass eine reelle positive Zahl x zwei reelle quadratische Wurzeln besitzt. Zum Beispiel haben wir für $x = 4$

$$\sqrt{4} = \pm 2.$$

Im Gegensatz dazu besitzen die negativen reellen Zahlen keine reelle Quadratwurzeln. Zum Beispiel gibt es kein $x \in \mathbb{R}$ sodass

$$x^2 = -5.$$

Durch die Einführung von komplexen Zahlen haben wir diese „Asymmetrie“ ausgeglichen. Tatsächlich gibt es für jedes $x \in \mathbb{R} \setminus \{0\}$ zwei quadratische Wurzeln in $\mathbb{C}$

$$\begin{aligned} &\pm\sqrt{x} && \text{für} \quad x > 0, \\ &\pm i\sqrt{|x|} && \text{für} \quad x < 0. \end{aligned}$$

Darüberhinaus besitzt jede komplexe Zahl $z \neq 0$ zwei Quadratwurzeln. Mit (1.6) sieht man sofort, dass für $z = |z|\, e^{i\varphi}$ gilt

$$\sqrt{z} = \pm\sqrt{|z|}e^{i\varphi/2}.$$

1.1.4 Anwendung auf Polynomgleichungen

Betrachten wir eine Polynomgleichung zweiten Grades

$$ax^2 + bx + c = 0, \tag{1.7}$$

wobei a, b, c beliebige reelle Zahlen sind (mit $a \neq 0$). Da $a \neq 0$ ist, können wir (1.7) äquivalent umschreiben als

$$x^2 + b'x + c' = 0, \tag{1.8}$$

mit $b' = \frac{b}{a}$ und $c' = \frac{c}{a}$. Ferner, können wir (1.8) umschreiben als

$$\left(x + \frac{b'}{2}\right)^2 - \frac{b'^2}{4} + c' = 0,$$

und bekommen als Lösungen

$$x_{1,2} = -\frac{b'}{2} \pm \sqrt{\frac{b'^2}{4} - c'} = \frac{-b' \pm \sqrt{b'^2 - 4c'}}{2}.$$

Ausgedrückt durch a, b, c haben wir

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

1.2 Begriff eines Körpers

Hier werden wir den Begriff des Zahlensytems axiomatisieren.

Definition 1.2. Eine Menge K heißt ein Körper, wenn sie mit folgenden zusätzlichen Strukturen ausgestattet ist:

1. **Addition:** Diese ist eine Abbildung

$$K \times K \to K \tag{1.9}$$
$$(a, b) \mapsto a + b, \tag{1.10}$$

für welche gelte

$$a + b = b + a \qquad \textit{(Kommutativität)}$$
$$(a + b) + c = a + (b + c) \qquad \textit{(Assoziativität)}$$

Ferner existiere ein Element $\mathbf{0} \in K$ für welches gilt

$$a + \mathbf{0} = a \qquad \forall a \in K. \tag{1.11}$$

Dieses Element wird Null-Element oder Null genannt.

Weiter muss für jedes $a \in K$ ein Element $a' \in K$ existieren, für welches gilt

$$a + a' = \mathbf{0}.$$

Dieses a' wird üblicherweise mit $-a$ bezeichnet und Inverses oder Negatives von a genannt.

2. **Multiplikation:** Diese ist eine Abbildung

$$K \times K \to K \tag{1.12}$$
$$(a, b) \mapsto a \cdot b, \tag{1.13}$$

für welche gelte

$$a \cdot b = b \cdot a \qquad \textit{(Kommutativität)}$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad \textit{(Assoziativität)}$$

Ferner, existiere ein Element $\mathbf{1} \in K \setminus \{0\}$ für welches gilt

$$a \cdot \mathbf{1} = a \qquad \forall a \in K. \tag{1.14}$$

Dieses Element wird Eins-Element oder Eins genannt.

Weiter muss für jedes $a \in K \setminus \{0\}$ ein Element $a' \in K$ existieren, für welches gilt

$$a \cdot a' = \mathbf{1}.$$

Dieses a' wird üblicherweise mit a^{-1} bezeichnet und multiplikatives Inverses von a genannt.

3. **Kompatibilität von Addition und Multiplikation:**

Für alle $a, b, c \in K$ gelte

$$(a + b) \cdot c = a \cdot c + b \cdot c \qquad \textit{(Distributivität)}.$$

Bemerkung 1.3. Sei K ein Körper.

(i) Sei 0 ein Null-Element (es existiert nach Definition), d.h. für jedes $a \in K$ gilt $a+0 = a$. Dann, nach Kommutativität der Addition, haben wir $0+a = a$ für jedes $a \in K$. Ähnlich gilt für ein Eins-Element 1, dass $1 \cdot a = a$ für jedes $a \in K$.

(ii) Es gibt nur ein Null-Element und nur ein Eins-Element, diese werden durch 0 bzw. 1 bezeichnet und die Null und die Eins gennant (Übung).

(iii) Die additiven und multiplikativen Inversen sind eindeutig definiert (Übung). Also sind die Bezeichnungen $-a$ und a^{-1} wohldefiniert.

(iv) Nach Definition können die Eins und die Null nicht gleich sein. Also hat jeder Körper K mindestens zwei Elemente.

(v) Für jedes $a \in K$ gilt $0 \cdot a = 0$ (Übung).

Beispiel 1.4.

1. Alle drei Mengen

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

mit der üblichen Null und Eins sind Körper, und die Mengeninklusionen sind mit der Addition und Multiplkation verträglich.

2. $\mathbb{Z}$ ist kein Körper, da die nicht alle multiplikative Inverse existieren.

3. Betrachten wir die Untermenge von $\mathbb{C}$ der Form

$$\mathbb{Q}(i) = \big\{a + bi \,|\, a, b \in \mathbb{Q}\big\},$$

und benutzen als Addition und Multiplikation diejenige der komplexen Zahlen.

Das einzige was wir zeigen müssen ist die Existenz von multiplikativen Inversen. Nach Formel (1.4) gilt für eine komplexe Zahl $a + bi$

$$(a + bi)^{-1} = \frac{a - ib}{a^2 + b^2},$$

und man sieht, dass $(a + bi)^{-1} \in \mathbb{Q}(i)$ für ein $(a + bi) \in \mathbb{Q}(i)$ gilt. Also ist $\mathbb{Q}(i)$ ein Körper.

4. $\mathbb{F}_2$

Betrachten wir eine zweielementige Menge

$$K = \{0, 1\},$$

und definieren die Addition durch

$$\begin{aligned} 0 + 0 &= 0, \\ 0 + 1 = 1 + 0 &= 1, \\ 1 + 1 &= 0, \end{aligned}$$

und die Multiplikation durch

$$\begin{aligned} 0 \cdot 0 &= 0, \\ 0 \cdot 1 = 1 \cdot 0 &= 0, \\ 1 \cdot 1 &= 1. \end{aligned}$$

Es ist leicht zu sehen, dass diese zwei Operationen K zu einem Körper machen. Dieser Körper wird üblicherweise mit $\mathbb{F}_2$ bezeichnet.

5. Restklassen modulo n.

   Sei R_n die Menge von Divisionsresten bezüglich einer positiven ganzen Zahl $n \geq 2$, d.h. wir haben

   $$R_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

   Die Menge R_n ist mit Addition und Multiplikation ausgestattet, die von $\mathbb{Z}$ induziert werden. D.h. wenn man die Summe von $\bar{a}$ und $\bar{b}$ ausrechnen möchte, nimmt man die entsprechenden ganzen Zahlen a und b, rechnet die Summe $a + b$ aus, und dann nimmt den Divisionsrest von $a + b$ durch n als die Ergebnis für $\bar{a} + \bar{b}$. Analog für die Multiplikation.

   R_2: In diesem Fall bekommen wir den zweielementigen Körper $\mathbb{F}_2$.

   R_3: Dies ist ein Körper mit drei Elementen $\mathbb{F}_3$.

   R_4: Es gilt $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$, also ist R_4 kein Körper!

2 12.04.18 — Vektorräume

Definition 2.1. Sei K ein Körper (z.B. $K = \mathbb{R}$). Eine Menge V heißt ein Vektorraum über K, wenn sie mit folgenden Strukturen ausgestattet ist:

1. **Addition:** Diese ist eine Abbildung

$$\begin{aligned} V \times V &\to V \\ (x, y) &\mapsto x + y, \end{aligned}$$

für welche gelte

$$\begin{aligned} x + y &= y + x && \textit{(Kommutativität)} \\ (x + y) + z &= x + (y + z) && \textit{(Assoziativität)} \end{aligned}$$

Ferner existiere ein Element $\mathbf{0} \in V$ für welches gilt

$$x + \mathbf{0} = a \qquad \forall x \in V.$$

Dieses Element wird Null-Element oder Null genannt.

Weiter muss für jedes $x \in V$ ein Element $x' \in V$ existieren, für welches gilt

$$x + x' = \mathbf{0}.$$

Dieses x' wird üblicherweise mit $-x$ bezeichnet und Inverses oder Negatives von x genannt.

2. **Skalarmultiplikation:** Diese ist eine Abbildung

$$K \times V \to V \tag{2.1}$$
$$(a, x) \mapsto a \cdot x, \tag{2.2}$$

für welche gelte

$$\begin{aligned} a \cdot (b \cdot x) &= (ab) \cdot x \\ 1 \cdot x &= x. \end{aligned}$$

3. **Kompatibilität von Addition und Skalarmultiplikation:**

Für alle $a, b \in K$ und $x, y \in V$ gelte die Distributivität

$$\begin{aligned} (a + b) \cdot x &= a \cdot x + b \cdot x, \\ a \cdot (x + y) &= a \cdot x + a \cdot y. \end{aligned}$$

Bemerkung 2.2.

1. Elemente von V nennt man Vektoren und Elemente von K Skalare.
2. Das Null-Element ist eindeutig definiert, d.h. es gibt nur eine Null.
3. Es gilt $0 \cdot x = 0$ für alle $x \in V$.

Beispiel 2.3.

1. Die Ebene $\mathbb{R}^2$ ist ein Vektorraum über $\mathbb{R}$. Allgemeiner ist $\mathbb{R}^n$, ausgestattet mit komponentenweiser Addition und Skalarmultiplikation, ein Vektorraum über $\mathbb{R}$.
2. Auf dieselbe Weise ist K^n ein Vektorraum über K für beliebigen Körper K.
3. Die Körperinklusion $\mathbb{Q} \subset \mathbb{R}$ stattet $\mathbb{R}$ mit der Struktur eines Vektorraumes über $\mathbb{Q}$ aus. Dasselbe gilt für $\mathbb{Q} \subset \mathbb{C}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(i)$ und auch jede beliebige andere Körperinklusion.
4. Über einem beliebigen Körper K gibt es der Vektorraum $V = \{0\}$.
5. Sei X eine Menge und $Funkt(X, \mathbb{R})$ die Menge aller Funktionen auf X mit Werten in $\mathbb{R}$, d.h. die Menge aller Abbildungen $X \to \mathbb{R}$. Man sieht leicht, dass die Menge $Funkt(X, \mathbb{R})$ ausgestattet mit der üblichen punktenweisen Addition von Funktionen und punktenweisen Multiplikation mit Elementen von $\mathbb{R}$ ein Vektorraum über $\mathbb{R}$ ist. Man kann hier $\mathbb{R}$ durch einen beliebigen Körper ersetzen.
6. Die Menge aller Polynome mit Koeffizienten in K ist ein K-Vektorraum.

Definition 2.4. Seien K ein Körper und V ein Vektorraum über K (z.B. $K = \mathbb{R}$ und $V = \mathbb{R}^2$). Vektoren $x_1, \ldots, x_n \in V$ heißen linear abhängig, wenn es $a_1, \ldots, a_n \in K$ gibt, nicht alle gleichzeitig Null, so dass

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0.$$

Wenn solche $a_1, \ldots, a_n$ nicht existieren, dann heißen $x_1, \ldots, x_n$ linear unabhängig.

Beispiel 2.5.

1. $V = \mathbb{R}^2$, $x = (1, 0)$, $y = (0, 1)$, $z = (2, 3)$. Vektoren x, y, z sind linear abhängig. Je zwei von den drei sind linear unabhängig.
2. $V = \mathbb{R}[x]$, alle $e_i = x^i$ sind linear unabhängig.
3. $V = \mathbb{R}$ als $\mathbb{Q}$-Vektorraum. Die Vektoren $x = \sqrt{2}$ und $y = \frac{1}{\sqrt{2}}$ sind linear abhängig. Die Vektoren $x = \sqrt{3}$ und $y = \sqrt{2}$ sind linear unabhängig. (Übungsblatt)

Definition 2.6. Ein K-Vektorraum V heißt endlichdimensional, wenn es eine $N \in \mathbb{Z}_{\geq 0}$ gibt, sodass für alle $n > N$ beliebige $x_1, \ldots, x_n \in V$ linear abhängig sind. Das kleinste solche N nennt man die Dimension von V und bezeichnet es mit $\dim V$.

Vektoren $x_1, \ldots, x_n \in V$ heißen eine Basis von V, wenn sie linear unabhängig sind und es für jedes $z \in V$ eindeutige $a_1, \ldots, a_n \in K$ gibt, so dass

$$z = a_1 x_1 + \cdots + a_n x_n$$

gilt.

Lemma 2.7. *Sei V ein Vektorraum über K von Dimension N.*

1. *Es existiert eine Basis mit N Elementen.*
2. *Jede Basis hat N Elemente.*

Beweis. 1. Klar, sonst wäre die Dimension kleiner. 2. Ohne Beweis. ■

Beispiel 2.8.

1. Seien $V = K^n$ und $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ für $1 \leq i \leq n$. Die Elemente $e_1, \ldots, e_n$ bilden eine Basis, die man Standardbasis von K^n nennt. Die Dimension von V ist n.
2. $\dim_{\mathbb{R}} \mathbb{C} = 2$
3. Betrachten wir den $\mathbb{R}$-Vektorraum

   $$V = \{P(x) \in \mathbb{R}[x] \mid \deg P(x) \leq n\}.$$

   Die Polynome $1, x, x^2, \ldots, x^n$ bilden eine Basis, $\dim V = n + 1$.
4. Ist $V = \mathbb{R}[x]$ endlichdimensional?

Definition 2.9. Seien V und W zwei Vektorräume über einem Körper K. Eine Abbildung

$$f \colon V \to W$$

heißt linear, wenn gilt

$$f(x + y) = f(x) + f(y),$$
$$f(ax) = af(x).$$

Beispiel 2.10.

1. $K, V = W$ beliebig, $f(x) = x$ ist linear.
2. K, V, W beliebig, $f(x) = 0$ ist linear.
3. $K, V = W$ beliebig, $a \in K$, $f(x) = ax$ ist linear.

4. $V = \mathbb{R}^2$, $W = \mathbb{R}$, $f(a,b) = a$ ist linear, $g(a,b) = a^2$ ist nicht linear.

5. $V = W = \mathbb{R}[x]$, $P(x) \mapsto P'(x)$ ist linear, d.h. die Ableitung ist linear.

6. $V = Funkt(\mathbb{R}, \mathbb{R})$, $W = \mathbb{R}$, $a \in \mathbb{R}$, $f \mapsto f(a)$ ist linear, d.h. die Auswertung an einem Punkt ist linear.

7. Seinen X eine Menge, W ein Vektorraum über K, $V = Funkt(X, W)$, $P \in X$, $f \mapsto f(P)$ ist linear.

3 18.04.18 — Matrizen

Definition 3.1. Sei K ein Körper. Eine $m \times n$-Matrix über K (d.h. mit Einträgen in K) ist eine rechteckige Tabelle

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})$$

mit m Zeilen, n Spalten, und $a_{ij} \in K$. Die Menge aller $m \times n$-Matrizen über K bezeichnen wir mit

$$Mat_{m,n}(K).$$

Man definiert folgende Operationen für Matrizen.

1. **Addition:** Seien $A = (a_{ij})$ und $B = (b_{ij})$ Matrizen aus $Mat_{m,n}(K)$. Dann definiert man deren Summe als
$$A + B = (a_{ij} + b_{ij}).$$

2. **Skalarmultiplikation:** Seien $a \in K$ und $B = (b_{ij}) \in Mat_{m,n}(K)$. Dann definiert man das Produkt als
$$aB = (ab_{ij}).$$

3. **Matrizenmultiplikation:** Seien $A = (a_{ij}) \in Mat_{m,n}(K)$ und $B = (b_{ij}) \in Mat_{n,r}(K)$. Dann definiert man das Produkt $A \cdot B \in Mat_{m,r}(K)$ als

$$A \cdot B = \Big(\sum_{s=1}^{n} a_{is} b_{sj} \Big).$$

   Die Matrizenmultiplikation ist assoziativ, d.h. es gilt

$$(A \cdot B) \cdot C = A \cdot (B \cdot C),$$

   aber nicht kommutativ, d.h. allgemein haben wir $A \cdot B \neq B \cdot A$.

4. **Transposition:** Für ein $A = (a_{ij}) \in Mat_{m,n}(K)$ definiert man die transponierte Matrix $A^t \in Mat_{n,m}(K)$ als
$$A^t = (a_{ji}).$$

5. **Determinante:** Sei $A = (a_{ij}) \in Mat_{n,n}(K)$. Dann definiert man die Determinante als

$$\det(A) = \sum_{i_1,\ldots,i_n} (-1)^{inv(i_1,\ldots,i_n)} \, a_{1i_1} a_{2i_2} \ldots a_{ni_n},$$

wobei $i_1, \ldots, i_n$ eine Permutation von $1, \ldots, n$ ist, und $inv(i_1, \ldots, i_n)$ ist die Anzahl von Inversionen in der Pemutation.

Laplace Formel:

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+1} a_{1i} M_{1i},$$

wobei der Minor M_{ab} gegeben ist durch die Determinante der Matrix, die aus M durch Streichen der a-ten Zeile und b-ten Spalte entsteht.

Ein paar Eigenschaften:

$$\begin{aligned} \det(AB) &= \det(A)\det(B), \\ \det(A^t) &= \det(A), \\ \det(BA) &= \det(AB). \end{aligned}$$

6. **Inverse Matrix:** Sei $A = (a_{ij}) \in Mat_{n,n}(K)$. Dann definiert man die adjunkte[1] Matrix als
$$adj(A) = ((-1)^{i+j} M_{ij})^t.$$
Es gilt
$$A \cdot adj(A) = adj(A) \cdot A = \det(A)\,\mathrm{Id}_n.$$
Falls gilt $\det(A) \neq 0$, können wir die inverse Matrix A^{-1} als schreiben
$$A^{-1} = \frac{1}{\det(A)} adj(A).$$
Die inverse Matrix ist die eindeutige Matrix mit der Eigenschaft
$$A^{-1}A = AA^{-1} = \mathrm{Id}_n.$$

Beispiel 3.2. Anwendung auf lineare Gleichungssysteme.

3.1 Lineare Abbildungen als Matrizen

3.1.1

Betrachten wir eine K-lineare Abbildung

$$\psi \colon K^n \to K^m.$$

[1] In der Vorlesung wurde das Wort "adjungierte" verwendet. Ich bedanke mich bei dem unbekannten Studenten, der mich darauf hingewiesen hat.

Sei $e_1, \ldots, e_n$ (bzw. $f_1, \ldots, f_m$) die Standardbasis von K^n (bzw. von K^m). Wir definieren eine Matrix $A_\psi = (a_{ij}) \in Mat_{m,n}(K)$ durch

$$\psi(e_i) = \sum_{j=1}^{n} a_{ij} f_j.$$

Weiter identifizieren wir Elemente von K^n mit Matrizen mit einer Spalte, d.h. wir schreiben ein Element $(x_1, \ldots, x_n) \in K^n$ als die Matrix

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Dann ist es leicht zu sehen, dass die Abbildung ψ durch die Multiplikation mit A_ψ gegeben ist

$$\psi(x) = A_\psi \, x.$$

Umgekehrt, definiert jede Matrix aus $Mat_{m,n}(K)$ eine K-lineare Abbildung

$$\begin{aligned} \psi_A \colon K^n &\to K^m \\ x &\mapsto Ax. \end{aligned}$$

Dadurch erhalten wir eine lineare Bijektion

$$\begin{aligned} \mathrm{Hom}(K^n, K^m) &\to Mat_{m,n}(K) \\ \psi &\mapsto A_\psi \end{aligned}$$

Unter dieser Identifikation entspricht die Matrixmultiplikation der Komposition von linearen Abbildungen.

3.1.2

Sei V ein Vektorraum über K von Dimension n, $e_1, \ldots, e_n$ eine Basis. Dann kann man jedes $x \in V$ eindeutig als

$$x = \sum_i x_i e_i,$$

mit $x_i \in K$, schreiben. Dadurch bekommen wir eine bijektive lineare Abbildung

$$\begin{aligned} &V \to K^n \\ &x \mapsto (x_1, \ldots, x_n). \end{aligned}$$

3.1.3

Seien V, W zwei K-Vektorräume, $\dim V = n$, $\dim W = m$. Weiter betrachten wir eine lineare Abbildung

$$\varphi\colon V \to W.$$

Wir wählen eine Basis $e_1, \ldots, e_n$ in V und eine Basis $f_1, \ldots, f_m$ in W. Diese geben uns (siehe oben) Isomorpshismen

$$\alpha\colon V \to K^n,$$
$$\beta\colon W \to K^m.$$

Jetzt können wir das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ {\scriptstyle\alpha^{-1}}\uparrow\downarrow{\scriptstyle\alpha} & & {\scriptstyle\beta}\downarrow\uparrow{\scriptstyle\beta^{-1}} \\ K^n & \xrightarrow{\psi} & K^m \end{array}$$

betrachten und die Abbildung

$$\psi = \beta \circ \varphi \circ \alpha^{-1}\colon K^n \to K^m$$

definieren. Umgekehrt, gegeben eine lineare Abbildung $\psi \in \mathrm{Hom}(K^n, K^m)$, definieren wir eine lineare Abbildung $\varphi\colon V \to W$ durch

$$\varphi := \beta^{-1} \circ \psi_A \circ \alpha.$$

Diese Konstruktion liefert eine K-lineare Bijektion

$$\mathrm{Hom}(V, W) \to \mathrm{Hom}(K^n, K^m).$$

Ferner erhalten wir durch Komposition mit dem Isomorphismus $\mathrm{Hom}(K^n, K^m) \to Mat_{m,n}(K)$ den gewünschten Isomorphismus

$$\mathrm{Hom}(V, W) \to Mat_{m,n}(K).$$

4 19.04.18 — Gruppen I

4.1 Erste Definitionen

Definition 4.1. Ein Monoid ist ein Tripel $(M, \circ, e)$ bestehend aus einer Menge M, einer zweistelligen Verknüpfung

$$\begin{aligned} M \times M &\to M \\ (x, y) &\mapsto x \circ y \end{aligned}$$

und einem ausgezeichneten Element $e \in M$ mit den folgenden Eigenschaften:

M1 Assoziativität: $\forall x, y, z \in M \quad (x \circ y) \circ z = x \circ (y \circ z)$.

M2 Neutrales Element: $\forall x \in M \quad x \circ e = e \circ x = x$.

Beispiel 4.2.

1. $(\mathbb{Z}, +, 0)$. Mann kann hier $\mathbb{Z}$ auch durch $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_{\geq 0}, \mathbb{Q}_{\geq 0}, \mathbb{R}_{\geq 0}$ ersetzen. Wenn K ein Körper ist, dann ist $(K, +, 0)$ ein Monoid. Wenn V ein Vektorraum ist, dann ist $(V, +, 0)$ ein Monoid.
2. $(\mathbb{Z}, \cdot, 1)$. Mann kann hier $\mathbb{Z}$ auch durch $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_{>0}, \mathbb{Q}_{>0}, \mathbb{R}_{>0}$ ersetzen. Wenn K ein Körper ist, dann ist $(K, \cdot, 1)$ ein Monoid.
3. $(Mat_n(K), \cdot, \mathrm{Id}_n)$ ist ein Monoid.

Bemerkung 4.3. Man sieht leicht, dass es in einem Monoid nur ein Eins-Element geben kann. Seien e und e' zwei Eins-Elemente, dann gilt

$$e = e \circ e' = e'.$$

Lemma 4.4. *Seien $x_1, \ldots x_n$ beliebige Elemente eines Monoids. Dann führt jede "Klammerung" des Produktes $x_1 \circ \cdots \circ x_n$ zum selben Ergebnis.*

Beweis. Übung (folgt aus M1). □

Definition 4.5. Ein Monoid M heißt kommutativ, wenn $\forall x, y \in M$

$$x \circ y = y \circ x$$

gilt.

Üblicherweise wird die Zweistelligeverknüpfung für kommutative Monoide additiv geschriben ($x + y := x \circ y$) und für nicht kommutative Monoide multiplikativ ($xy := x \circ y$).

Das Produkt von n Kopien des selben Elementes $x \circ \cdots \circ x$ wird mit x^n bezeichnet. Es ist auch nützlich festzulegen $x^0 = e$. Man sieht leicht, dass es gilt

$$x^n \circ x^m = x^{n+m} \quad \forall n, m \in \mathbb{Z}_{\geq 0}.$$

Wenn die Verknüpfung additiv geschrieben wird, dann benutzt man nx anstatt von x^n. Dann wird die obige Formel zu $nx + mx = (n + m)x$.

Ein Element $x \in M$ heißt invertierbar, wenn es ein Element y gibt (Linksinverses), so dass gilt

$$y \circ x = e$$

und ein Element z gibt (Rechtsinverses), so dass gilt

$$x \circ z = e.$$

Lemma 4.6. *Falls x invertierbar ist, dann ist jedes Linksinverse zu x dem Rechtsinversen gleich.*

Beweis. $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = z$. ■

Also, für jedes invertierbares x gibt es ein eindeutiges Inverses, dass man mit x^{-1} (oder $-x$) bezeichnet. Weiter bezeichnen wir $(x^{-1})^n$ durch x^{-n}. Dann gilt

$$x^n \circ x^m = x^{n+m} \quad \forall n, m \in \mathbb{Z},$$

für ein invertierbares $x \in M$.

Definition 4.7. Eine Gruppe ist ein Monoid in dem jedes Element invertierbar ist.

Lemma 4.8. *Die Menge M^* der invertierbaren Elemente eines Monoids M ist eine Gruppe.*

Beweis. Man muss zeigen, dass das Produkt von zwei invertierbaren Elementen wieder invertierbar ist. Das folgt aus der Formel: $x \circ y \circ y^{-1} \circ x^{-1} = e$. ■

Beispiel 4.9.

1. $G = \{e\}$.
2. $(\mathbb{Z}, +)$ (Varianten: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$).
3. $(\mathbb{Q}^*, \cdot)$ (Varianten: $\mathbb{R}, \mathbb{C}, \dots$).
4. $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ und $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$.
5. Die Permutationsgruppe (oder symmetrische Gruppe) S_n.
6. $GL_n(K) = \{A \in Mat_n(K) \mid \det(A) \neq 0\}$.

7. $SL_n(K) = \{A \in Mat_n(K) \mid \det(A) = 1\}$.

Lemma 4.10. *Sei G eine Gruppe. Wenn gilt $x \circ y = x \circ z$ (oder $y \circ x = z \circ x$), dann gilt $y = z$.*

Beweis. Angenommen $x \circ y = x \circ z$ gilt. Dann können wir die beide Seiten der Gleichheit von links mit x^{-1} multiplizieren und bekommen $y = z$. ■

Definition 4.11. Eine Gruppe heißt kommutativ, wenn sie als Monoid kommutativ ist. Kommutative Gruppen nennt man öfters abelsche Gruppen und schreibt die Verknüpfung additiv.

Beispiel 4.12. Abelsch: $\mathbb{Z}, K, K^*, S^1, \mu_n$. Nicht abelsch: GL_n.

Definition 4.13. Sei G eine Gruppe. Eine Untergruppe von G ist eine nichtleere Teilmenge $H \subset G$, die das neutrale Element e enthält und bezüglich der induzierten Verknüpfung eine Gruppe ist.

Beispiel 4.14.

1. $n\mathbb{Z} \subset \mathbb{Z}$.
2. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
3. $\mathbb{Z}^* = \mu_2 \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.
4. $GL_n(\mathbb{Z}) \subset GL_n(\mathbb{Q}) \subset GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$.
5. $SL_n(K) \subset GL_n(K)$.

4.2 Homomorpshismen

Definition 4.15. Eine Abbildung von Gruppen (oder Monoide) $f\colon G \to H$ heißt Homomorphismus, wenn gilt

$$f(a \circ b) = f(a) \circ f(b) \quad \forall a, b \in G$$
$$f(e_G) = e_H.$$

Übung: Zeigen Sie, dass wir die Eigenschaft $f(e_G) = e_H$ für Gruppen weglassen können.

Beispiel 4.16.

1. $f\colon G \to H$, $f(a) = e_H$ für alle $a \in G$.
2. $\mathrm{id}_G\colon G \to G$ die Identität.
3. $\mathbb{Z} \to G$, $n \mapsto x^n$, für ein beliebiges $x \in G$.
4. $\exp\colon \mathbb{R} \to \mathbb{R}^*$.

5. $\det\colon GL_n(K) \to K^*$.

Lemma 4.17. *Die Komposition zweier Homomorpshimen ist ein Homomorphismus.*

Beweis. Klar. ■

Definition 4.18.

1. Monomorphismus = injektiver Homomorpshismus.
2. Epimorphismus = surjektiver Homomorpshismus.
3. Isomorphismus = bijektiver Homomorpshismus.
4. Endomorphismus = Homomorpshismus von $G \to G$.
5. Automorphismus = bijektiver Endomorpshismus.

Beispiel 4.19.

1. Betrachten wir den Homomorphismus
$$\begin{aligned}\mathbb{R} &\to S^1 = \{z \in \mathbb{C} \mid |z| = 1\}\\ \varphi &\mapsto e^{i\varphi}.\end{aligned}$$
Dieser ist ein Epi, aber kein Mono.
2. Betrachten wir
$$\begin{aligned}\mathbb{Z} &\to \mathbb{Z}\\ x &\mapsto 2x.\end{aligned}$$
Kein Epi, aber Mono.

Definition 4.20. Sei $f\colon G \to H$. Der Kern von f ist die Teilmenge von G definiert durch
$$Kerf = \{x \in G \mid f(x) = e\}.$$
Das Bild von f ist die Teilmenge von H definiert durch
$$Imf = \{y \in H \mid \exists x \in G\colon f(x) = y\}.$$

Lemma 4.21. *Man sieht leicht, dass der Kern bzw. das Bild eines Homomorphismus Untergruppen von G bzw. H sind.*

Beispiel 4.22.

1. $\det\colon GL_n(K) \to K^*$, $Ker\det = SL_n(K)$.
2. $S^1 \to S^1$, $z \mapsto z^n$, $Ker = \mu_n$.

Lemma 4.23. *Ein Homomorphismus $f\colon G \to H$ ist ein Mono $\iff$ $Kerf = \{e\}$. Ein Homomorphismus $f\colon G \to H$ ist ein Epi $\iff$ $Imf = H$.*

Beweis. Eine Richtung ist klar: wenn f ein Mono ist, dann gilt $Kerf = \{e\}$. Umgekehrt: wenn gilt $f(x) = f(y)$, dann $f(xy^{-1}) = e$, dann $xy^{-1} = e$. ■

5 25.04.18 — Gruppen II

5.1 Direktes Produkt

Seien $(M_1, \circ_1, e_1)$ und $(M_2, \circ_2, e_2)$ zwei Monoide. Dann kann das direkte Produkt

$$M_1 \times M_2 = \{(x_1, x_2) \mid x_i \in M_i\}$$

mit einer natürlichen Struktur eines Monoids ausgestattet werden

$$\begin{aligned}&(x_1, x_2) \circ (y_1, y_2) = (x_1 \circ y_1, x_2 \circ y_2),\\ &e = (e_1, e_2).\end{aligned}$$

Direktes Produkt von Gruppen wird auf dieselbe Weise definiert.

5.2 Relationen

Definition 5.1. Sei X eine Menge. Eine Relation R auf X ist eine Teilmenge $R \subset X \times X$. Man schreibt $x \sim_R y$, wenn $(x, y) \in R$.

Beispiel 5.2.

1. Sei X die Menge aller Studierenden in diesem Raum und
$$A \sim B \iff \text{A mag B.}$$
2. Sei $X = \mathbb{Z}$ und
$$a \sim b \iff a < b.$$
3. Sei $X = \mathbb{Z}$ und
$$x \sim y \iff x - y \in 2\mathbb{Z}.$$

Eine Relation heißt

1. reflexiv $\iff x \sim_R x \quad \forall x \in X$.
2. symmetrisch $\iff \quad x \sim_R y \iff y \sim_R x$.
3. transitiv $\iff$ wenn $x \sim_R y$ und $y \sim_R z$, dann $x \sim_R z$.

Definition 5.3. Eine Relation heißt Äquivalenzrelation, wenn sie reflexiv, symmetrisch und transitiv ist.

Beispiel 5.4. Untersuchen Sie dies für die obigen Beispiele.

Sei R eine Äquivalenzrelation relation auf einer Menge X. Für jedes $x \in X$ betrachtet man die Teilmenge

$$[x]_R = \{a \in X \mid a \sim x\},$$

die Äquivalenzklasse von x bezüglich R gennant wird. Es ist leicht zu sehen, dass gilt

$$[x]_R = [y]_R \iff y \in [x]_R.$$

Dadurch zerfällt die Menge X in eine disjunkte Vereinigung der Teilmengen der Form $[x]_R$.

Definition 5.5. Sei R eine Äquivalenzrelation auf X. Die Menge aller Äquivalenzklassen nennt man Quotient von X bezüglich R und bezeichnet sie mit X/R oder $X/\sim$.

Beispiel 5.6.

1. $X = \mathbb{Z}$, $x \sim y \iff x - y \in 2\mathbb{Z}$.
2. $X = \mathbb{Z}$, $x \sim y \iff x - y \in n\mathbb{Z}$. Denken Sie an die Menge der Divisionsresten aus der ersten Vorlesung R_n.

5.3 Gruppenwirkungen

Sei G eine Gruppe und X eine Menge. Eine Wirkung von G auf X ist ein Abbildung

$$\begin{aligned} &\sigma \colon G \times X \to X \\ &(g, x) \mapsto \sigma(g, x) = g \cdot x \end{aligned} \tag{5.1}$$

mit den folgenden Eigenschaften:

1. $\sigma(e, x) = x \quad \forall x \in X$;
2. $\sigma(g_1 g_2, x) = \sigma(g_1, \sigma(g_2, x))$.

Frage: kann man die erste Eigenschaft aus der zweiten folgern?

Beispiel 5.7.

1. $G = S_n$ wirkt auf $\{1, 2, \ldots, n\}$.
2. Für eine beliebige Gruppe G erfüllt das Produkt $G \times G \to G$ die Axiomen der Gruppenwirkung.
3. $GL_n(K)$ wirkt auf K^n.
4. $GL_n(K)$ wirkt auf Ursprungsgeraden (Unterverktorräume von Dimension 1) in K^n durch Matrizenmultiplikation von links.

Sei X eine Menge. Durch $Aut(X)$ werden wir die Gruppe aller bijektieven Abbildungen $X \to X$ bezeichnen.

Lemma 5.8. *Eine Gruppenwirkung* (5.1) *auf X wird äquivalent durch einen Gruppenhomomorpshimus*

$$\rho\colon G \to Aut(X) \tag{5.2}$$

gegeben.

Beweis. Gegeben (5.1), definieren wir (5.2) durch

$$g \mapsto \sigma(g, \cdot) \in Aut(X).$$

Das Inverse zu $\sigma(g, \cdot)$ ist durch $\sigma(g^{-1}, \cdot)$ gegeben. Also landet man tatsächlich in $Aut(X)$. Man sieht auch leicht, dass es ein Gruppenhomomorpshismus ist.

Umgekehrt, gegeben ein ρ wie in (5.2), definiert man

$$\sigma(g, x) = \rho(g)(x)$$

und bekommt ein σ wie in (5.1). ■

Definition 5.9. Betrachten wir eine Wirkung einer Gruppe G auf einer Menge X.

1. Für jedex $x \in X$ definiert man eine Untergruppe $Stab(x) \subset G$ als

   $$Stab(x) = \{g \in G \mid g \cdot x = x\}.$$

   Diese Untergruppe nennt man Stabilisator von x.

2. Für jedex $x \in X$ definiert man eine Teilmenge $Orb(x) \subset X$ als

   $$Orb(x) = \{y \in X \mid \exists g \in G : g \cdot x = y\}.$$

   Diese Teilmenge nennt man der Orbit oder die Bahn von x.

3. Die Wirkung heißt frei $\iff$ $Stab(x) = \{e\}$ $\forall x \in X$.

4. Die Wirkung heißt transitiv $\iff$ für jede $x, y \in X$ existiert ein $g \in G$, so dass $x = gy$.

6 26.04.18 — Gruppen III

Betrachten wir eine Wirkung von G auf X. Dann kann man eine Äquivalenzrelation auf X definieren.

$$x \sim y \iff \exists g \in G \colon y = gx.$$

Es ist leicht zu sehen, dass die Äquivalenzklassen genau die Bahnen sind. Den Quotienten von X bezüglich dieser Äquivalenzrelation bezeichnet man mit $G \setminus X$. Elemente von $G \setminus X$ sind Bahnen der Wirkung.

Bemerkung 6.1. Was oben definiert wurde nennt man präziser linke Wirkung von G auf X. Analog kann man auch eine rechte Wirkung als eine Abbildungen

$$\begin{aligned} X \times G &\to X \\ (x, g) &\mapsto x \cdot g, \end{aligned}$$

mit den Eigenschaften

$$\begin{aligned} x \cdot (g_1 g_2) &= (x \cdot g_1) \cdot g_2 \\ x \cdot e &= x \end{aligned}$$

definieren. Stabilisatoren, Bahnen, Freiheit und Transitivität werden auf die gleiche Weise definiert.

Beispiel 6.2. Seien $X = Mat_{m,n}(K)$, $G_1 = GL_m(K)$, $G_2 = GL_n(K)$. Die Gruppe G_1 wirkt von links auf X durch Matrizenmultiplikation. Analog, G_2 wirkt von rechts auf X.

6.1 Nebenklassen

Sei G eine Gruppe, $H \subset G$ eine Untergruppe. Betrachten wir eine Äquivalenzrelation definiert durch

$$x \sim_L y \iff \exists h \in H \colon xh = y.$$

Die Äquivalenzklassen bezüglich L nennt man Linksnebenklassen. Gegeben ein Element $x \in G$, wird seine Linksebenklasse mit xH bezeichnet. Explizit haben wir

$$xH = \{xh \mid h \in H\}.$$

Die Gruppe G zerfällt in eine disjunkte Vereinigung von H-Linksnebenklassen. Die Menge von H-Linksnebenklassen wird mit G/H bezeichnet.

Analog definiert man die Rechtsnebenklassen. D.h. man betrachtet stattdessen die Äquivalenzrelation

$$x \sim_R y \iff \exists h \in H \colon hx = y.$$

Gegeben ein Element $x \in G$, wird seine Rechtsnebenklasse mit Hx bezeichnet. Explizit haben wir

$$Hx = \{hx \mid h \in H\}.$$

Die Gruppe G zerfällt in eine disjunkte Vereinigung von H-Rechtsnebenklassen. Die Menge von H-Rechtsnebenklassen wird mit $H \setminus G$ bezeichnet.

Beispiel 6.3. Sei $G = \mathbb{Z}$.

1. Jede Untergruppe von $\mathbb{Z}$ ist der Form $n\mathbb{Z}$ für $n \geq 0$.
2. Die Linksnebenklassen von $n\mathbb{Z}$ sind

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Bemerkung 6.4. Man kann die H-Nebenklassen als Bahnen einer Wirkung von H auf G betrachten: für Linksnebenklassen nimmt man die rechte Wirkung von H auf G durch Multiplikation, für Rechtsnebenklassen die linke Wirkung.

Satz 6.5 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe und $H \subset G$ eine Untergruppe. Dann gilt*

$$|G| = |H| \cdot |G/H|.$$

Beweis. Alle Nebenklassen haben die gleiche Anzahl von Elementen und sind dusjunkt. ■

Lemma 6.6. *Betrachten wir eine transitive Wirkung von G auf X. Für jedes $P \in X$ können wir eine surjektive Abbildung definieren*

$$\begin{aligned} f_P \colon G &\to X \\ g &\mapsto g \cdot P, \end{aligned}$$

die eine Bijektion

$$\begin{aligned} G/Stab(P) &\to X \\ gStab(P) &\mapsto g \cdot P \end{aligned}$$

induziert.

Beweis. Die Surjektivität folgt aus der Transitivität. Die Injektivität:

$$g_1 \cdot P = g_2 \cdot P \Rightarrow g_2^{-1} g_1 \in Stab(P). \blacksquare$$

6.2 Normalteiler

Lemma 6.7. *Sei $H \subset G$ eine Untergruppe. Die folgenden Aussagen sind äquivalent:*

1. *$\forall g \in G$ gilt $gHg^{-1} = H$.*
2. *$\forall g \in G$ und $\forall h \in H$ gilt $ghg^{-1} \in H$.*
3. *$\forall g \in G$ gilt $gH = Hg$.*
4. *H-Linksnebenklassen und H-Rechtsnebenklassen sind gleich.*

Beweis. 3. $\iff$ 4. ist offensichtlich; 1. $\iff$ 2. gezeigt an der Tafel; der Rest als Übung gelassen. ■

Definition 6.8. Eine Untergruppe $H \subset G$ heißt normal (oder Normalteiler), wenn eine der äquivalenten Aussagen des Lemmas 6.7 gilt.

Beispiel 6.9.

1. Das Zentrum $Z(G) = \{g \in G \mid \forall h \in G\colon hgh^{-1} = g\}$ ist ein Normalteiler (Übungsblatt).
2. Jede Untergruppe einer abelschen Gruppe ist normal.
3. $SL_n(K) \subset GL_n(K)$ ist normal (siehe nächstes Lemma).
4. $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset GL_2(K)$ ist kein Normalteiler. (Übung)

Lemma 6.10. *Sei $\psi\colon G \to H$ ein Gruppenhomomorpshismus. Dann ist $Ker\,\psi$ ein Normalteiler.*

Beweis. Folgt sofort aus dem Lemma 6.7.2. ■

7 02.05.18 — Gruppen IV

7.1 Faktorgruppen

Es sei G eine Gruppe und $U \subset G$ eine Untergruppe. Wie zuvor bezeichnen wir die Menge der U-Linksnebenklassen von U in G mit G/U.

Definition 7.1. Sei nun $N \subset G$ ein Normalteiler. Wir definieren eine Gruppenstruktur auf G/N durch die Verknüpfung

$$\begin{aligned} G/N \times G/N &\to G/N \\ (g_1N) * (g_2N) &= (g_1g_2)N. \end{aligned}$$

Diese ist wegen $((g_1N) * (g_2N)) * (g_3N) = (g_1N) * ((g_2N) * (g_3N))$ assoziativ, die Eins ist gegeben durch eN, und für $gN \in G/N$ ist $g^{-1}N$ ein Inverses. Die Gruppe G/N wird **Quotient**, oder auch **Faktorgruppe**, von G modulo N genannt.

Bemerkung 7.2.

1. Im Folgenden werden wir statt $*$ wieder $\cdot$ schreiben (oder das Verknüpfungssymbol ganz weglassen). Für die Nebenklassen verwenden wir oft auch die etwas kürzere Notation $[g] \coloneqq gN$ für $g \in G$.

2. Für die Wohldefiniertheit der Verknüpfung aus Definition 7.1 ist entscheidend, dass $N \subset G$ ein Normalteiler ist: Dies bedeutet nach Lemma 6.7.(3) ja nicht anderes als dass links- und rechts-Nebenklassen von N gleich sind, also $gN = Ng$ für alle $g \in G$. Insbesondere gibt es also für alle $n \in N$, $g \in G$, ein $\tilde{n} \in N$ mit $ng = g\tilde{n}$ (nämlich $\tilde{n} = g^{-1}ng \in N$). Betrachten wir dann $g_1N = g_1'N$ (also $g_1' = g_1n_1$ für ein $n_1 \in N$) und $g_2N = g_2'N$ (also $g_2' = g_2n_2$ für ein $n_2 \in N$), für $g_1, g_1', g_2, g_2' \in G$, so gilt

$$(g_1'N)(g_2'N) = (g_1'g_2')N = (g_1n_1g_2n_2)N = (g_1g_2\tilde{n}_1n_2)N = (g_1g_2)N = (g_1N)(g_2N).$$

3. Nach Definition der Gruppenverknüpfung auf G/N ist die Abbildung

$$\begin{aligned} \pi\colon G &\longrightarrow G/N \\ g &\longmapsto gN. \end{aligned}$$

ein Gruppenhomomorphismus, der als **kanonische Projektion** (oder auch kanonische Surjektion) auf die Faktorgruppe bezeichnet wird. Man sieht sofort, dass π surjektiv ist und $\ker(\pi) = N$ gilt.

7.2 Einige wichtige Sätze der elementaren Gruppentheorie

Satz 7.3 (Homomorphiesatz)**.** *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann ist*

$$\begin{aligned} \overline{f}\colon G/\ker(f) &\longrightarrow H, \\ [g] &\longmapsto f(g) \end{aligned}$$

ein wohldefinierter, injektiver Gruppenhomomorphismus. Insbesondere ist

$$\overline{f}\colon G/\ker(f) \longrightarrow \operatorname{Im}(f)$$

ein Gruppenisomorphismus.

Beweis. Zur Wohldefiniertheit: Bekanntlich gilt für $g, g' \in G$, dass

$$[g] = [g'] \in G/\ker(f) \iff \exists h \in \ker(f)\colon g' = gh.$$

Also $\overline{f}([g']) = f(g') = f(gh) = f(g)f(h) \overset{h\in\ker(f)}{=} f(g) = \overline{f}([g])$. Nach Definition der Gruppenstruktur auf $G/\ker(f)$ ist klar, dass $\overline{f}$ ein Homomorphismus ist. Der Kern von $\overline{f}$ ist

$$\begin{aligned}\ker(\overline{f}) =& \{[g] \in G/\ker(f) \mid \overline{f}([g]) = f(g) = e_H\}\\ =& \{[g] \in G/\ker(f) \mid g \in \ker(f)\} = \{[e_G]\},\end{aligned}$$

d. h. $\overline{f}$ ist injektiv. Nach Definition von $\overline{f}$ gilt $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$, also

$$G/\ker(f) \xrightarrow[\overline{f}]{\simeq} \operatorname{Im}(\overline{f}) = \operatorname{Im}(f).$$

□

Bemerkung 7.4. Genau wie im obigen Beweis lässt sich zeigen: Ist $f\colon G \to H$ ein Gruppenhomomorphismus und $N \subset G$ ein Normalteiler mit $N \subset \ker(f)$, so ist

$$\overline{f}\colon G/N \longrightarrow H, \quad \overline{f}([g]) = f(g)$$

ein wohldefinierter Gruppenhomomorphismus.

Beispiel 7.5.

1. Der Gruppenhomomorphismus

   $$\mathbb{R} \longrightarrow \mathbb{C} \setminus \{0\}, \quad \varphi \longmapsto e^{2\pi i\varphi}$$

   induziert einen Isomorphismus

   $$\mathbb{R}/\mathbb{Z} \longrightarrow S^1.$$

2. Sei $0 < n \in \mathbb{N}$ und K ein Körper. Der Gruppenhomomorphismus

   $$\det\colon \mathrm{GL}_n(K) \longrightarrow K \setminus \{0\}, \quad M \longmapsto \det(M)$$

   induziert einen Isomorphismus

   $$\overline{\det}\colon \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \longrightarrow K \setminus \{0\}.$$

Satz 7.6 (Korrespondenzsatz)**.** *Es sei G eine Gruppe und $N \subset G$ ein Normalteiler. Weiter sei $\mathcal{U} := \{U \subset G \text{ Untergruppe} \mid N \subset U\}$ die Menge der Untergruppen von G, die N enthalten und $\mathcal{V} := \{V \subset G/N \text{ Untergruppe}\}$ die Menge der Untergruppen von G/N. Die kanonische Surjektion $\pi\colon G \to G/N$ ist von oben bekannt. Die folgenden Abbildungen sind zueinander invers und definieren damit eine Bijektion $\mathcal{U} \simeq \mathcal{V}$:*

$$\begin{aligned} a\colon \mathcal{U} &\longrightarrow \mathcal{V}, \quad U \longmapsto \pi(U) \\ b\colon \mathcal{V} &\longrightarrow \mathcal{U}, \quad V \longmapsto \pi^{-1}(V) \end{aligned}$$

Beide Abbildungen bilden Normalteiler auf Normalteiler ab, d. h. es gilt

$$U \subset G \text{ Normalteiler} \quad \Longleftrightarrow \quad \pi(U) \subset G/N \text{ Normalteiler}$$

für alle $U \in \mathcal{U}$.

Beweis. Da π ein Gruppenhomomorphismus ist, ist $\pi(U) \subset G/N$ eine Untergruppe für jedes $U \in \mathcal{U}$, a ist also wohldefiniert. Für die Wohldefiniertheit von b wollen wir zeigen, dass auch $\pi^{-1}(V) \subset G$ wieder eine Untergruppe ist für jedes $V \in \mathcal{V}$ (nachdem $e_G N \in V$ für jede Untergruppe $V \subset G/N$ gelten muss, ist $N = \pi^{-1}(e_G N) \subset \pi^{-1}(V)$ klar). Seien dazu $g, h \in \pi^{-1}(V)$ beliebig. Dann gilt $\pi(gh) = \pi(g)\pi(h) \in V$, also $gh \in \pi^{-1}(V)$. Außerdem ist natürlich $\pi(e_G) = e_G N \in V$, also $e_G \in \pi^{-1}(V)$, und für ein beliebiges $g \in \pi^{-1}(V)$ gilt $\pi(g^{-1}) = \pi(g)^{-1} \in V$, also $g^{-1} \in \pi^{-1}(V)$. Es bleibt noch zu zeigen, dass $a \circ b = \mathrm{id}_{\mathcal{V}}$ und $b \circ a = \mathrm{id}_{\mathcal{U}}$ gilt. Sei dazu zuerst $V \in \mathcal{V}$ beliebig. Dann ist zu zeigen

$$a \circ b(V) = \pi(\pi^{-1}(V)) = V.$$

Die Inklusion "$\subset$" ist dabei klar und gilt für Abbildungen beliebiger Mengen, die Inklusion "$\supset$" gilt, da π surjektiv ist. Für ein beliebiges $U \in \mathcal{U}$ ist dagegen zu zeigen, dass

$$b \circ a(U) = \pi^{-1}(\pi(U)) = U$$

gilt. Die Inklusion "$\supset$" ist dabei wieder klar, für die Inklusion "$\subset$" überlegen wir uns Folgendes: Es sei $g \in \pi^{-1}(\pi(U))$ beliebig. Dann gilt

$$\begin{aligned} g \in \pi^{-1}(\pi(U)) &\Longleftrightarrow gN = \pi(g) \in \pi(U) \\ &\Longleftrightarrow \exists u \in U\colon gN = uN = \pi(u) \\ &\Longleftrightarrow \exists n \in N\colon g = un \\ &\overset{N \subset U}{\Longrightarrow} g \in U. \end{aligned}$$

Schließlich beobachten wir noch, dass gilt

$$\begin{aligned} \mathcal{U} \ni U \subset G \text{ Normalteiler} &\Longleftrightarrow \forall g \in G\colon gUg^{-1} = U \\ &\Longrightarrow \forall\ gN = \pi(g) \in G/N\colon gN\pi(U)(gN)^{-1} = \pi(gUg^{-1}) = \pi(U). \end{aligned}$$

und

$$\begin{aligned}\mathcal{V} \ni V \subset G/N \text{ Normalteiler } &\iff \forall gN \in G/N\colon (gN)V(gN)^{-1} = V\\ &\implies \forall g \in G,\ \forall u \in \pi^{-1}(V)\colon \pi(gug^{-1}) = \pi(g)\pi(u)\pi(g)^{-1}) \in V\\ &\iff \pi^{-1}(V) \subset G \text{ Normalteiler.}\end{aligned}$$

□

Beispiel 7.7. Vgl. Übung.

Sei nun eine Gruppe G gegeben und $N, H \subset G$ Untergruppen. Ist N normal in G, so definieren wir die Untergruppe

$$N \cdot H \coloneqq \{nh \,|\, n \in N,\ h \in H\} \subset G.$$

1. Offensichtlich ist $e_G \in N \cdot H$.
2. Wie schon zuvor verwendet, gilt, da N ein Normalteiler ist, für alle $n \in N$ und alle $h \in H$ (sogar alle $h \in G$), dass es ein $\tilde{n} \in N$ gibt mit $nh = h\tilde{n}$ (und natürlich umgekehrt, d. h. $hn = \hat{n}h$ für ein $\hat{n} \in N$). Damit erhalten wir für $n_1, n_2 \in N$ und $h_1, h_2 \in H$, dass
$$(n_1h_1)(n_2h_2) = n_1h_1n_2h_2 = n_1\tilde{n}_2h_1h_2 \in N \cdot H.$$
3. Ebenso erhalten wir für $n \in N$, $h \in H$, dass
$$(nh)^{-1} = h^{-1}n^{-1} = \widehat{n^{-1}}h^{-1} \in N \cdot H.$$

Ganz genauso lässt sich natürlich $H \cdot N \coloneqq \{hn \,|\, h \in H,\ n \in N\} \subset G$ definieren, und $N \cdot H = H \cdot N$.

Satz 7.8 (Isomorphiesätze)**.** *Sei G eine Gruppe.*

(I1) Ist $H \subset G$ eine Untergruppe und $N \subset G$ ein Normalteiler, dann sind $N \cap H \subset H$ und $N \subset N \cdot H$ Normalteiler und es existiert ein kanonischer Isomorphismus

$$H/(N \cap H) \xrightarrow{\simeq} N \cdot H/N.$$

(I2) Sind $H \subset N \subset G$ Untergruppen, so dass $H, N \subset G$ Normalteiler sind, so ist auch $N/H \subset G/H$ ein Normalteiler und es existiert ein kanonischer Isomorphismus

$$G/N \xrightarrow{\simeq} (G/H)/(N/H).$$

Beweis. (I1). Dass $N \subset N \cdot H$ ein Normalteiler ist, ist klar. Wir betrachten den Gruppenhomomorphismus

$$\begin{aligned} f\colon H &\longrightarrow N \cdot H \longrightarrow N \cdot H/N, \\ h &\longmapsto e_G h \longmapsto (e_G h)N. \end{aligned}$$

Dieser ist surjektiv, denn für jedes $(nh)N \in N \cdot H/N$ gilt ja

$$(nh)N = (ne_G)N \cdot (e_G h)N = e_G hN = f(h).$$

Nach dem Homomorphiesatz genügt es damit, zu beobachten:

$$\ker(f) = \{h \in H \mid hN = (e_G h)N = e_G N \in N \cdot H/N\} = \{h \in H \mid h \in N\} = N \cap H.$$

(I2). Nach dem Korrespondenzsatz ist klar, dass $N/H \subset G/H$ ein Normalteiler ist. Wir betrachten den Gruppenhomomorphismus

$$\begin{aligned} f\colon G &\longrightarrow G/H \longrightarrow (G/H)/(N/H), \\ g &\longmapsto gH \longmapsto [gH]. \end{aligned}$$

Dieser ist offensichtlich surjektiv, so dass es nach dem Homomorphiesatz wiederum genügt, zu beobachten:

$$\ker(f) = \{g \in G \mid [gH] = [e_G H]\} = \{g \in G \mid gH \in N/H\} = N.$$

□

Beispiel 7.9.

1. Für $G = \mathbb{Z}$, $H = 10\mathbb{Z}$ und $N = 15\mathbb{Z}$:

$$5\mathbb{Z}/15\mathbb{Z} = (10\mathbb{Z} + 15\mathbb{Z})/15\mathbb{Z} \simeq 10\mathbb{Z}/(10\mathbb{Z} \cap 15\mathbb{Z}) = 10\mathbb{Z}/30\mathbb{Z}.$$

2. Für $G = \mathbb{Z}$, $N = 5\mathbb{Z}$ und $H = 10\mathbb{Z}$:

$$(\mathbb{Z}/10\mathbb{Z})/(5\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}.$$

8 03.05.18 — Gruppen V

8.1 Zyklische Gruppen

Es sei G eine Gruppe und $M \subset G$ eine Teilmenge. Wir bezeichnen mit $\langle M \rangle \subset G$ die eindeutige kleinste Untergruppe von G, die M enthält.

Lemma 8.1. *Die Untergruppe $\langle M \rangle \subset G$ ist in der Tat eindeutig bestimmt.*

Beweis. Es seien $U_1, U_2 \subset G$ zwei Untergruppen von G, die beide M enthalten. Dann ist offenbar auch $U_1 \cap U_2$ eine solche Untergruppe. □

Bemerkung 8.2. Die Untergruppe $\langle M \rangle$ besteht aus allen Elementen in G der Form

$$m_1^{i_1} m_2^{i_2} \cdots m_n^{i_n}, \quad n \in \mathbb{N},\ m_j \in M,\ i_j \in \{\pm 1\} \text{ für alle } j = 1, \ldots, n.$$

Insbesondere ist hier natürlich $m_i = m_j$ für $i \neq j$ zugelassen, das neutrale Element $e \in G$ entspricht dem Fall $n = 0$.

Notation 8.3. Ist $M = \{m_1, \ldots, m_n\}$ für ein $n \in \mathbb{N}$, so schreiben wir auch

$$\langle m_1, \ldots, m_n \rangle \coloneqq \langle M \rangle.$$

Definition 8.4. Für eine Gruppe G und ein Element $g \in G$ heißt die Ordnung $|\langle g \rangle|$ der von g erzeugten Untergruppe von G die **Ordnung** von g.

Bemerkung 8.5. Insbesondere ist also nach dem Satz 6.5 (Satz von Lagrange) für jede endliche Gruppe G (also $|G| < \infty$) die Ordnung aller Elemente ein Teiler von $|G|$.

Definition 8.6. Eine Gruppe heißt **zyklisch**, wenn ein $g \in G$ existiert, so dass $G = \langle g \rangle$ gilt.

Beispiel 8.7.

1. $\mathbb{Z} = \langle 1 \rangle$.
2. $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$.
3. Nach dem Satz von Lagrange ist jede Gruppe G mit $|G| = p$, für eine Primzahl p, zyklisch.

Lemma 8.8. *Es sei $G = \langle g \rangle$ eine zyklische Gruppe. Dann ist jede Untergruppe von G wieder zyklisch. Ist $|G| = n$, so existiert zu jedem Teiler $m|n$ genau eine Untergruppe $U \subset G$ mit $|U| = m$.*

Beweis. Es sei $U \subset G$ eine Untergruppe. Wir setzen $u \coloneqq g^a$ mit

$$a = \min\{a \in \mathbb{Z}_{>0} \mid g^a \in U\}.$$

Dann ist $U = \langle u \rangle$, denn angenommen, es gäbe ein $h \in G \setminus U$, dann wäre nach Voraussetzung ja $h = g^b$ für ein $0 \neq b \in \mathbb{Z}$. Da ja auch h^{-1} in U liegen muss, können wir ohne Einschränkung

der Allgemeinheit davon ausgehen, dass $b > 0$ gilt. Nun könnten wir eine Division mit Rest ausführen:

$$b = qa + r \quad \text{mit } r = |r| < a.$$

Damit ist aber

$$U \ni h = g^b = g^{qa+r} = (g^a)^q g^r \quad \Longleftrightarrow \quad g^r = h(g^a)^{-q} \in U,$$

ein Widerspruch zur Minimalität von a.

Nun sei $|G| = n$ und $m|n$ ein Teiler der Gruppenordnung. Offensichtlich ist $U_m \coloneqq \langle g^{n/m} \rangle$ eine Untergruppe der Ordnung m. Sei weiter U eine beliebige Untergruppe der Ordnung m. Wie wir bereits gesehen haben, ist U wieder zyklisch, sagen wir, $U = \langle g^x \rangle$ für ein $x \in \mathbb{Z}_{>0}$. Nach Voraussetzung muss die Ordnung von g^x gerade m sein, insbesondere also $(g^x)^m = e_G$, d. h. $n|xm$. Damit haben können wir schreiben $x = y\frac{n}{m}$, für ein $y \in \mathbb{Z}_{>0}$, das heißt $g^x \in U_m$, also $U \subset U_m$. Wegen $|U| = m = |U_m|$ gilt aber folglich schon $U = U_m$. □

Beispiel 8.9. Ist $G = \langle g \rangle$ eine zyklische Gruppe, so ist

$$f \colon \mathbb{Z} \longrightarrow G, \quad n \mapsto g^n$$

ein surjektiver Gruppenhomomorphismus. Der Kern ist die zyklische Untergruppe $\langle n \rangle = n\mathbb{Z} \subset \mathbb{Z}$, nach dem Homomorphiesatz ist also

$$\overline{f} \colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} G$$

ein Isomorphismus, d. h. bis auf Isomorphie ist jede zyklische Gruppe von der Form $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. Insbesondere ist also jede zyklische Gruppe abelsch.

8.2 Symmetrische Gruppen

Wir wollen zuerst die folgende Bezeichnung einführen:

$$\Delta_n \coloneqq \{1, 2, \ldots, n\}$$

Definition 8.10. Die **symmetrische Gruppe** S_n ist definiert als

$$S_n \coloneqq \mathrm{Aut}(\Delta_n) = (\{f \colon \Delta_n \to \Delta_n \text{ bijektiv}\}, \circ),$$

also als die Menge der bijektiven Abbildungen auf Δ_n mit der Komposition solcher Abbildungen als Verknüpfung. Die Elemente von S_n werden als **Permutationen** (von n Elementen) bezeichnet.

Bemerkung 8.11. Es ist $|S_n| = n!$.

Notation 8.12.

1. Wir stellen ein Element $\sigma \in S_n$ dar als

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

2. Ein Element τ von S_n heißt k-**Zykel** (oder auch Zykel der Länge k), wenn es paarweise verschiedene Elemente $\{x_1, \dots, x_k\} \subset \Delta_n$ gibt, so dass gilt

$$\tau(x_i) = x_{i+1} \quad \text{für } i < k,$$
$$\tau(x_k) = x_1.$$

   Wir notieren einen solchen Zykel in etwas kompakterer Schreibweise als

$$(x_1, x_2, \dots, x_k).$$

   Nach Definition gilt offenbar

$$(x_1, x_2, \dots, x_k) = (x_2, \dots, x_k, x_1). \tag{8.1}$$

   Die Ordnung eines k-Zykels ist gerade k. Zwei Zykel $\tau = (x_1, \dots, x_k)$, $\rho = (y_1, \dots, y_l)$ in S_n heißen **disjunkt**, wenn die zugrundeliegenden Mengen $\{x_1, \dots, x_k\}$ und $\{y_1, \dots, y_l\}$ disjunkt sind. Sind $\tau, \rho \in S_n$ disjunkte Zykel, so gilt offensichtlich $\tau \circ \rho = \rho \circ \tau$.

3. Ein Zykel der Länge 2 wird eine **Transposition** genannt.

8.3 Eigenschaften symmetrischer Gruppen

Satz 8.13. *1. Jedes Element $\sigma \in S_n$ lässt sich eindeutig (bis auf Reihenfolge der Faktoren) als Produkt disjunkter Zykel schreiben.*

2. Jedes Element $\sigma \in S_n$ ist ein Produkt von Transpositionen, das heißt

$$S_n = \langle T \rangle \quad \textit{für } T = \{(a, b) \mid 1 \le a < b \le n\} \textit{ die Menge der Transpositionen.}$$

Beweis. Zu a). Wir betrachten die von $\sigma \in S_n$ erzeugte Untergruppe $\langle \sigma \rangle \in S_n$. Diese wirkt definitionsgemäß auf der Menge Δ_n, durch

$$\langle \sigma \rangle \times \Delta_n \longrightarrow \Delta_n, \quad (\sigma, i) \longmapsto \sigma(i).$$

Es sei $\{x_1, \dots, x_r\}$ ein Repräsentantensystem dieser Wirkung, das heißt, Δ_n zerfällt disjunkt in die Bahnen $B_i \coloneqq \mathrm{Orb}(x_i)$, $i = 1, \dots, r$. Wir bezeichnen die Längen dieser Bahnen mit $\lambda_i \coloneqq |B_i|$, $i = 1, \dots, r$. Dann ist

$$\sigma = \prod_{i=1}^{r} (x_i, \sigma(x_i), \sigma^2(x_i), \dots, \sigma^{\lambda_i - 1}(x_i)), \tag{8.2}$$

wobei die Reihenfolge der Faktoren beliebig vertauschbar ist. Aufgrund der Eigenschaft (8.1) von Zykeln ist diese Darstellung offensichtlich unabhängig von der Wahl der Repräsentanten der Bahnen. Umgekehrt legt eine Darstellung der Form (8.2) die Permutation σ eindeutig fest.
Zu b). Nach a) genügt es offenbar, zu zeigen, dass jeder Zykel ein Produkt von Transpositionen ist. Für einen beliebigen Zykel $(x_1, x_2, \ldots, x_k) \in S_n$ gilt aber

$$(x_1, x_2, \ldots, x_k) = (x_1, x_2) \circ (x_2, x_3) \circ \ldots \circ (x_{k-1}, x_k). \tag{8.3}$$

□

Beispiel 8.14.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 8 & 5 & 4 & 6 & 1 & 11 & 9 & 2 & 10 & 7 \end{pmatrix} = (1, 3, 5, 6) \circ (2, 8, 9) \circ (7, 11).$$

Korollar 8.15. *1. Für jedes $n \geq 2$ ist*

$$S_n = \langle (1, 2), (1, 2, \ldots, n) \rangle = \langle (i, i+1), (1, 2, \ldots, n) \rangle,$$

für ein beliebiges $i \in \{1, \ldots, n-1\}$.

2. Ist $n = p$ eine Primzahl, so ist

$$S_p = \langle \tau, (1, 2, \ldots, p) \rangle = \langle \tau, \sigma \rangle,$$

für eine beliebige Transposition $\tau \in S_p$ und einen beliebigen p-Zykel $\sigma \in S_p$.

Beweis. Übung. Zeige, dass sich alle Transpositionen erzeugen lassen, verwende dazu $\sigma \circ (x_1, \ldots, x_k) \circ \sigma^{-1} = (\sigma(x_1), \ldots, \sigma(x_k))$ für $\sigma \in S_n$ und einen k-Zykel $(x_1, \ldots, x_k)$. □

Definition 8.16. Für eine Permutation $\sigma \in S_n$ setzen wir

$$\operatorname{sgn}(\sigma) := \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}. \tag{8.4}$$

Man nennt $\operatorname{sgn}(\sigma)$ das **signum** der Permutation $\sigma \in S_n$.

Satz 8.17. *1. Das Signum* sgn *definiert einen Gruppenhomomorphismus*

$$\operatorname{sgn}\colon S_n \longrightarrow \{\pm 1\}.$$

2. Ist $\tau = (x_1, \ldots, x_k) \in S_n$ ein k-Zykel, so gilt $\operatorname{sgn}(\tau) = (-1)^{k-1}$.

Definition 8.18. Der Kern des Signum-Homomorphismus',

$$A_n := \ker(\operatorname{sgn}) = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} \subset S_n,$$

wird **alternierende Gruppe** genannt.

9 09.05.18 — Ringe I

Teil 1. Ringe und Homomorphismen

Definition 9.1. Ein Ring ist ein Tupel $(R, +, \circ, 0, 1)$ bestehend aus einer Menge R, zweistelligen Verknüpfungen $+$ (Addition) und $\circ$ (Multiplikation) und Elementen $0, 1 \in R$ mit den folgenden Eigenschaften:

R1 $(R, +, 0)$ ist eine abelsche Gruppe.

R2 $(R, \circ, 1)$ ist ein Monoid.

R3 Distributivität: für alle $a, b, c \in R$ gilt

$$a \circ (b + c) = a \circ b + a \circ c,$$
$$(b + c) \circ a = b \circ a + c \circ a.$$

Ein Ring heißt kommutativ, wenn $(R, \circ, 1)$ ein kommutativer Monoid ist.

Bemerkung 9.2. Wie früher sind die Eins und die Null eindeutig definiert.

Beispiel 9.3.

1. $(\mathbb{Z}, +, \cdot)$.
2. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.
3. $(K, +, \cdot)$ für einen Körper K.
4. Sei X eine Menge und $Funkt(X, \mathbb{R})$ die Menge aller Funktionen auf X mit Werten in $\mathbb{R}$

   $$Funkt(X, \mathbb{R}) \coloneqq \{f \colon X \to \mathbb{R}\}.$$

   Man definiert die Addition und die Multiplikation punktenweise

   $$(f + g)(P) = f(P) + g(P),$$
   $$(f \cdot g) = f(P)g(P),$$

   wobei $P \in X$ ein beliebiger Punkt ist. Das Tupel $(Funkt(X, \mathbb{R}), +, \cdot)$ ist ein Ring. Die Null ist die Nullfunktion und die Eins ist die Einsfunktion.
5. Der Nullring: $R = \{0\}$.

Lemma 9.4. *Sei R ein Ring. Dann gilt für jedes $x \in R$*

$$x \cdot 0 = 0 \cdot x = 0.$$

Beweis. Wir haben

$$x = x \cdot 1 = x \cdot (1 + 0) = x \cdot 1 + x \cdot 0 = x + x \cdot 0.$$

Jetzt subtrahieren wir auf beiden Seiten x und bekommen $0 = x \cdot 0$. □

Definition 9.5. Ein Ring R mit $0 \neq 1$ heißt ein Divisionsring, wenn jedes $x \in R \setminus \{0\}$ bezüglich der Multiplikation invertierbar ist. In diesem Fall ist $R^* := R \setminus \{0\}$ eine Gruppe. Ein Körper ist ein kommutativer Divisionsring.

Bemerkung 9.6. Diese Definition eines Körpers ist äquivalent zu Definition 1.2 (Übung).

Definition 9.7. Ein Ringhomomorpshismus $f\colon R \to S$ ist eine Abbildung mit den Eigenschaften

$$\begin{aligned} f(a + b) &= f(a) + f(b), \\ f(a \cdot b) &= f(a) \cdot f(b), \\ f(1_R) &= 1_S. \end{aligned}$$

Das heißt, Ringhomomorphismen sind Homomorphismen von zugrundeliegenden Additiven Gruppen bzw. Monoide.

Beispiel 9.8.

1. Die natürliche Mengeninklusionen $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sind Ringhomomorpshismen.
2. Seien $R = Funkt(X, \mathbb{R})$, $S = \mathbb{R}$ und $P \in X$. Die Auswertung einer Funktion f im Punkt P

$$\begin{aligned} R &\to S \\ f &\mapsto f(P) \end{aligned}$$

   ist ein Ringhomomorpshismus.

Definition 9.9. Sei R ein Ring. Eine Teilmenge $S \subset R$ heißt Unterring, wenn

1. $S \subset R$ ist eine Untergruppe bezüglich der Addition,
2. $S \cdot S \subset S$,
3. $1_R \in S$.

Beispiel 9.10.

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
2. $\mathbb{Z}$ hat keine Unterringe.
3. $\cdots \subset C^2(\mathbb{R}, \mathbb{R}) \subset C^1(\mathbb{R}, \mathbb{R}) \subset Funkt(\mathbb{R}, \mathbb{R})$. Hier $C^n(\mathbb{R}, \mathbb{R})$ ist der Ring von n-mal stetig differenzierbaren Funktionen auf $\mathbb{R}$ mit Werten in $\mathbb{R}$.

Definition 9.11. Sei R ein Ring und $I \subset R$ eine Untergruppe bezüglich der Addition. Die Teilmenge I heißt ein Linksideal, wenn gilt $R \cdot I \subset I$, und ein Rechtsideal, wenn gilt $I \cdot R \subset I$. Wenn I gleichzeitig ein Links- und ein Rechtsideal ist, dann sagt man, dass I ein zweiseitiges Ideal ist.

Bemerkung 9.12.

1. Ein (Links-, Rechts- oder zweiseitiges) Ideal $I \subset R$ ist genau dann ein Unterring von R, wenn gilt $I = R$.

2. Wenn R kommutativ ist, dann ist jedes Linksideal auch ein Rechtsideal. In diesem Fall sind also alle drei Begriffe äquivalent.

Beispiel 9.13.

1. Die Teilmengen $I = \{0\}$ und $I = R$ sind immer zweiseitige Ideale.

2. In einem Körper K gibt es keine Ideale außer $I = \{0\}$ und $I = K$.

3. Alle Ideale in $\mathbb{Z}$ sind der Form $n\mathbb{Z}$.

4. Sei X eine Menge und $P \in X$ ein Punkt. Die Menge

$$\{f \in Funkt(X, \mathbb{R}) \mid f(P) = 0\}$$

ist ein Ideal.

10 16.05.18 — Ringe II

Teil 1. fortgesetzt

Definition 10.1. Der Kern eines Ringhomomorphismus' $f\colon R \to S$ ist die Teilmenge

$$\operatorname{Ker} f = \{a \in R \mid f(a) = 0\} \subset R.$$

Das Bild eines Ringhomomorphismus' $f\colon R \to S$ ist die Teilmenge

$$\operatorname{Im} f = \{b \in S \mid b = f(a),\, a \in R\} \subset S.$$

Lemma 10.2. *Der Kern eines Ringhomomorphismus' $f\colon R \to S$ ist ein zweiseitiges Ideal und das Bild ist ein Unterring.*

Beweis. 1. Kern: Seien $a, b \in \operatorname{Ker} f$, dann gilt

$$f(a+b) = f(a) + f(b) = 0 + 0 = 0.$$

Also ist $Kerf$ eine Untergruppe von R bezüglich der Addition.
Seien $x \in \operatorname{Ker} f$ und $a \in R$. Dann gilt

$$f(ax) = f(a)f(x) = 0 = f(xa).$$

Also sind ax und xa auch in $\operatorname{Ker} f$, d.h. $IR \subset I$ und $RI \subset I$.

2. Bild: Übung. □

Lemma 10.3. *Sei $f\colon R \to S$ ein Ringhomomorphismus. Dann gilt:*

1. *f ist injektiv $\iff$ $Ker\, f = \{0\}$.*
2. *f ist surjektiv $\iff$ $Im\, f = S$.*

Beweis. 1. Wir müssen zeigen: $f(a) = f(b) \iff a = b$. Also betrachten wir $a, b \in R$ mit der Eigenschaft $f(a) = f(b)$. Dann gilt

$$f(a) = f(b) \iff f(a-b) = 0 \iff a - b \in \operatorname{Ker} f.$$

2. Klar. □

Sei R ein Ring und $S \subset R$ ein Unterring. Man kann die Inklusion $S \subset R$ als eine Abbildung $S \to R$ auffassen. Auf diese Weise sieht man, dass jeder Unterring von R als Bild eines Ringhomomorpshismus' ensteht. Wir werden zeigen, dass auch jedes zweiseitiges Ideal der Kern eines Ringhomomorpshismus' ist.

Definition 10.4. Sei $I \subset R$ ein zweiseitiges Ideal. Da die additive Gruppe eines Ringes abelsch ist, ist I ein Normalteiler von R. Also ist der Quotient R/I eine abelsche Gruppe bezüglich der Addition. Explizit ist die Addition durch die Formel

$$(a+I)+(b+I)=(a+b)+I \tag{10.1}$$

gegeben (nach Definition 7.1). Wir definieren eine Multiplikation auf R/I durch

$$(a+I)\cdot(b+I) \coloneqq (ab)+I. \tag{10.2}$$

Lemma 10.5. *Die Multiplikation (10.2) ist wohldefiniert.*

Beweis. Wir müssen zeigen, dass für beliebige $\tilde{a} \in a+I$ und $\tilde{b} \in b+I$ gilt $\tilde{a}\tilde{b} \in (ab)+I$. Man kann solche $\tilde{a}$ und $\tilde{b}$ schreiben als

$$\tilde{a}=a+x\,, \quad \tilde{b}=b+y$$

mit $x, y \in I$. Dann haben wir

$$\tilde{a}\tilde{b}=(a+x)(b+y)=ab+(xb+ay+xy).$$

Da I ein zweiseitiges Ideal ist, liegt $xb+ay+xy$ in I und wir sind fertig. □

Theorem 10.6. *(i) Die Menge R/I mit der Addition (10.1) und mit der Multiplikation (10.2) ist ein Ring. Man nennt diesen Ring* Faktorring *oder* Quotientenring*. (ii) Die kanonische Projektion $f\colon R \to R/I$, $a \mapsto a+I$ ist ein Epimorpshismus mit Ker $f = I$.*

Beweis. Erstens folgt aus Definition 7.1 sofort, dass R/I bez. der Addition (10.1) eine abelsche Gruppe ist. Zweitens ist R/I ein Monoid bez. der Multiplikation (10.2):

$$((a+I)(b+I))(c+I)=(ab+I)(c+I)=(ab)c+I=a(bc)+I=(a+I)(bc+I)=(a+I)((b+I)(c+I)),$$
$$(1+I)(a+I)=1a+I=a+I\,, \quad (a+I)(1+I)=a1+I=a+I.$$

Letztendlich ist (10.2) distributiv:

$$\begin{aligned}((a+I)+(b+I))(c+I)&=((a+b)+I)(c+I)=(a+b)c+I=\\&=(ac+bc)+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I).\end{aligned}$$

Die zweite Aussage ist klar. □

11 17.05.18 — Ringe III

Teil 1. fortgesetzt

Theorem 11.1. *Sei $f\colon R \to S$ ein Ringhomomorphismus. Dann gibt es einen natürlichen Isomorphismus*

$$R/Ker\ f \to Im\ f.$$

Beweis. Sei $I = \text{Ker } f$. Der Homomorpshismus wird durch die Formel

$$\begin{aligned} \bar{f}\colon R/I &\to \text{Im } f \\ a + I &\mapsto f(a). \end{aligned}$$

definiert. Dieser ist wohldefiniert und bijektiv (Übung). □

Korollar 11.2. *Sei $f\colon R \to S$ ein Ringhomomorphismus.*

1. *f Epi $\implies$ $S \cong R/Ker\ f$.*
2. *Jedes f lässt sich kanonisch als die Komposition*

$$R \to R/Ker\ f \to Im\ f \to S$$

schreiben.

Beweis. Folgt aus dem obigen Theorem. □

Satz 11.3 (Korrespondenzsatz für Ideale)**.** *Sei R ein Ring und $I \subset R$ ein zweiseitiges Ideal. Dann induziert die kanonische Projektion $\psi\colon R \to R/I$ eine Bijektion zwischen Linksidealen in R/I und Linksidealen in R, die I enthalten*

$$J \mapsto \psi^{-1}(J).$$

Analog hat man ähnliche Bijektion für Rechtsideale und zweiseitige Ideale.

Beweis. Ähnlich zu Satz 7.6. Übungsblatt. □

Teil 2. Kommutative Ringe, maximale Ideale und Primideale

Beispiel 11.4 (Polynomringe)**.** Polynomringe und deren Faktorringe sind die wichtigste Beispiele für kommutative Ringe.

1. Sei R ein kommutativer Ring (z.B. $R = \mathbb{Z}$ oder $R = \mathbb{Q}$) und x eine Variable (ein Buchstabe). Ein Polynom in der Variable x und mit Koeffizienten in R ist ein Ausdruck der Form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

wobei $a_i \in R$ beliebige Elemente sind. Man definiert die Summe und das Produkt von Polynomen auf die übliche Weise. Man sieht leicht, dass die Menge aller Polynome mit dieser Addition und Multiplikation einen Ring bilden, den wir mit $R[x]$ bezeichnen.

2. Polynomringe in mehreren Variablen kann man induktiv definieren

$$R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n].$$

Explizit bedeutet es, dass ein Element von $R[x_1, \ldots, x_n]$ eine endliche Summe der Form

$$\sum_{I=(i_1,\ldots,i_n)} a_I x_1^{i_1} \ldots x_n^{i_n}$$

ist.

Warnung: Sei K ein Körper und $P(x) \in K[x]$ ein Polynom. Für jedes $a \in K$ kann man $P(x)$ in diesem Punkt auswerten. Auf diese Weise erhalten wir eine Funktion $K \to K$. Es kann aber passieren, dass für zwei unterschiedliche Polynome die dazugehörige Funktionen gleich sind (vgl. Übungsblatt).

Definition 11.5.

1. Seien $I, J \subset R$ zwei Ideale. Dann definieren wir die Summe $I + J$ als

$$I + J = \{a + b \in R \mid a \in I, b \in J\}.$$

Man sieht leicht, dass $I + J$ das kleinste Ideal ist, welches I und J enthält.

2. Seien $I, J \subset R$ zwei Ideale. Dann definieren wir das Produkt IJ als

$$IJ = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I, b_i \in J, n \in \mathbb{Z}_{\geq 1}\}.$$

3. Sei $M \subset R$ eine Teilmenge. Dann bezeichnet man mit (M) das kleinste Ideal in R, welches M enthält. Explizit können wir es wie folgt beschreiben

$$(M) = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R, a_i \in M, n \in \mathbb{Z}_{\geq 1}\}.$$

4. Für $M = \{m_1, \ldots, m_n\}$ schreiben wir

$$(m_1, \ldots, m_n) := (M).$$

5. Für $M = \{m\}$ heißt das Ideal (m) Hauptideal. Explizit haben wir

$$(m) = \{rm \mid r \in R\}.$$

Definition 11.6. Sei R ein Ring und $I \subset R$ ein echtes Ideal.

1. I heißt maximal $\iff$ es gibt kein echtes Ideal, das I enthält.
2. I heißt prim $\iff$ (wenn $xy \in I$, dann gilt $x \in I$ oder $y \in I$).

Lemma 11.7. *Jedes maximales Ideal ist prim.*

Beweis. Seien $I \subset R$ ein maximales Ideal und $x, y \in R$ mit $xy \in I$. Nehmen wir an, dass $x \notin R$ (sonst wären wir schon fertig). Dann gilt

$$I \subset I + Rx = R.$$

Also haben wir

$$1 = a + bx,$$

mit $a \in I$ und $b \in R$. Durch Multiplizieren mit y bekommen wir $y = ay + bxy \in I$. □

Lemma 11.8. *$I \subset R$ maximal $\iff$ $R/\mathfrak{m}$ ist ein Körper.*

Beweis. In einem Körper gibt es keine nichttriviale Ideale (d.h. die einzige Ideale sind (0) und R).[2] Also es genügt zu zeigen, dass in $R/\mathfrak{m}$ keine nichttriviale Ideale gibt.

Nach Satz 11.3 etnsprechen die Ideale in $R/\mathfrak{m}$ eins-zu-eins mit Idealen in R, die das Ideal $\mathfrak{m}$ enthalten. Nach Definition des maximalen Ideals sind die einzige solche Ideale $\mathfrak{m}$ und R, die in $R/\mathfrak{m}$ den trivialen Idealen (0) und $R/\mathfrak{m}$ entsprechen. □

Beispiel 11.9. Sei $R = \mathbb{Z}$. Dann ist jedes Ideal der Form $n\mathbb{Z}$. Wir haben

$$n\mathbb{Z} \subset m\mathbb{Z} \iff m \text{ teilt } n.$$

Also ist $p\mathbb{Z} \subset \mathbb{Z}$ in keinem echten Ideal enthalten. Daraus folgt, dass $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ ein Körper ist (vgl. Übungsblatt). Der Körper $\mathbb{F}_p$ wird endlicher Körper mit p Elementen gennant.

Definition 11.10. Sei R ein kommutativer Ring.

1. Ein Element $x \neq 0$ aus R heißt Nullteiler $\iff$ $\exists\, y \neq 0$ aus R sodass $xy = 0$.
2. Der Ring R heißt Integritätsbereich $\iff$ es gibt keine Nullteiler in R und $0 \neq 1$.

Beispiel 11.11.

1. $\mathbb{Z}$ ist ein Integritätsbereich.
2. Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein Integritätsbereich.
3. Sei K ein Körper. Dann ist $K[x]/(x^2)$ kein Integritätsbereich, da die Klasse von x in $K[x]/(x^2)$ ein Nullteiler ist.
4. Das Nullideal $(0) \subset R$ ist prim $\iff$ R ist Integritätsbereich.

[2] Übungsblatt 6, Aufgabe 5.b.

12 23.05.18 — Ringe IV

Teil 2. fortgesetzt

Lemma 12.1. *Ein Ideal $I \subset R$ ist prim $\iff$ R/I ist Integritätsbereich.*

Beweis. Seien $x + I$ und $y + I$ zwei Elemente in R/I. Dann gilt

$$(x + I)(y + I) = xy + I.$$

$\Rightarrow$) Nehmen wir an, dass I prim ist. Dann gilt:

$$(x + I)(y + I) = I \iff xy \in I \Rightarrow x \in I \text{ oder } y \in I.$$

Also ist entweder $x + I = I$ oder $y + I = I$.

$\Leftarrow$) Nehmen wir an, dass R/I ein Integritätsbereich ist. D.h. aus $(x + I)(y + I) = I$ folgt $x \in I$ oder $y \in I$. Dann ist I ein Primideal.

□

Definition 12.2. Sei M eine Menge.

1. Eine partielle Ordnung auf M ist eine Relation $\leq$, die reflexiv, transitiv und antisymmetrisch ist.
2. Eine partielle Ordnung heißt total $\iff \forall x, y \in M\ x \leq y$ oder $y \leq x$.
3. Ein Element $x \in M$ heißt größtes Element $\iff a \leq x\ \forall a \in M$.
4. Ein Element $x \in M$ heißt maximal $\iff x \leq a$ impliziert $a = x$.
5. Ein Element $x \in M$ heißt obere Schranke für eine Teilmenge $N \subset M \iff a \leq x$ $\forall a \in N$.

Beispiel 12.3. Teilmengen einer Menge bez. Inklusion. Varianten: Untergruppen einer Gruppe, Ideale eines Ringes.

Bemerkung 12.4. Gibt es ein größtes Element, so ist dieses zugleich das einzige maximale Element. Im Allgemeinen existiert kein solches größtes Element und es gibt viele maximale Elemente.

Lemma 12.5 (Lemma von Zorn)**.** *Sei P eine partiell geordnete Menge, in der jede total geordnete Teilmenge(=eine Kette) eine obere Schranke hat. Dann enthält P mindestens ein maximales Element.*

Beweis. Bosch, Lemma 5, §3.4. □

Lemma 12.6. *Sei $I \subset R$ ein echtes Ideal. Dann existiert ein maximales Ideal $\mathfrak{m} \subset R$, sodass $I \subset \mathfrak{m} \subset R$.*

Beweis. Wir werden das Lemma von Zorn anwenden. Als Menge P nehmen wir die Menge aller echten Ideale in R, die das Ideal I enthalten. Diese Menge ist halbgeordnet bezüglich der Mengeninklusion. Um das Lemma von Zorn anwenden zu können genügt es zu zeigen, dass es für jede Kette von Idealen

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$$

ein echtes Ideal $\mathfrak{a}$ mit der Eigenschaft $\forall\, i\, \mathfrak{a}_i \subset \mathfrak{a}$ gibt. Nehmen wir als $\mathfrak{a}$ die Vereinigung

$$\mathfrak{a} := \cup_i \mathfrak{a}_i.$$

Jetzt müssen wir zeigen, dass: 1) $\mathfrak{a}$ ist ein Ideal; 2) $\mathfrak{a} \neq R$.

1. Betrachten wir $x, y \in \mathfrak{a}$. Dann gilt $x \in \mathfrak{a}_i$ und $y \in \mathfrak{a}_j$ für gewisse i und j. Dann gilt auch $x, y \in \mathfrak{a}_k$ mit $k = max(i, j)$. Dann für die Summe haben wir $x + y \in \mathfrak{a}_k \subset \mathfrak{a}$. Analog zeigt man, dass $rx \in \mathfrak{a}\ \forall r \in R$. Also ist $\mathfrak{a}$ ein Ideal.

2. Nehmen wir an, dass gilt $\mathfrak{a} = R$. Dann gilt $1 \in \mathfrak{a}$. Also gibt es ein i, sodass $1 \in \mathfrak{a}_i$. Dann ist $\mathfrak{a}_i$ kein echtes Ideal. Widerspruch!

□

Beispiel 12.7. Maximale Ideale in $\mathbb{Z}$ sind der Form (p) für eine Primzahl p.

Korollar 12.8. *Jedes nicht invertierbare Element x eines Ringes R liegt in einem maximalen Ideal.*

Beweis. Das Hauptideal (x) betrachten und das obige Lemma anwenden. □

Teil 3. Hauptidealringe

Sei R ein kommutativer Ring. Laut Definition 11.5 heißt ein Ideal $I \subset R$ ein Hauptideal, wenn es ein Element $x \in R$ gibt, sodass

$$I = (x) := \{ax \mid a \in R\}.$$

Definition 12.9. Sei R ein Ring mit $0 \neq 1$.

1. R heißt Hauptidealring $\iff$ jedes Ideal ist ein Hauptideal.

2. R heißt Hauptidealbereich $\iff$ R ist ein Hauptidealring und ein Integritätsbereich.

Beispiel 12.10. $\mathbb{Z}$ ist ein Hauptidealbereich.

Definition 12.11. Man sagt, dass in einem Ring R eine Division mit Rest existiert, wenn es eine Funktion $\varphi\colon R \to \mathbb{Z}_{\geq 0}$ gibt, sodass

1. $\varphi^{-1}(0) = \{0\}$;
2. $\forall a, b \in R,\ b \neq 0,\ \exists q, r \in R : a = qb + r$ und $\varphi(r) < \varphi(b)$.

Beispiel 12.12.

1. $\mathbb{Z}$ mit $\varphi(n) = |n|$.
2. $K[x]$ mit $\varphi(P(x)) = \deg(P(x)) + 1$, $\deg(0) = -1$.

Lemma 12.13 (Polynomdivision)**.** *Seien K ein Körper und $A(x), B(x)$ Polynome aus $K[x]$ mit $B(x) \neq 0$. Dann existieren eindeutige Polynome $Q(x), R(x) \in K[x]$, sodass*

$$A(x) = Q(x)B(x) + R(x),$$

mit $\deg(R(x)) < \deg(B(x))$.[3]

Beweis. Übungsblatt. □

Lemma 12.14. *Ein Ring mit Division mit Rest ist ein Hauptidealring.*

Beweis. Sei $I \subset R$ ein Ideal. OBDA: $I \neq (0)$. Sei $b \neq 0 \in I$ ein Element mit der Eigenschaft $\varphi(b) = min\{\varphi(x) \mid x \in I, x \neq 0\}$. Dann gilt $I = (b)$. Tatsächlich können wir jedes Element $a \in I$ schreiben als $a = qb + r$ mit $\varphi(r) < \varphi(b)$. Da $r \in I$ und $\varphi(b)$ minimal ist, bekommen wir $r = 0$ und $a \in (b)$. □

Korollar 12.15. *$\mathbb{Z}$ und $K[x]$ sind Hauptidealbereiche.*

[3] Hier wird durch $\deg(P(x))$ der Grad von $P(x)$ bezeichnet. Wir setzen $\deg(0) = -1$.

13 24.05.18 — Ringe V

Teil 3. fortgesetzt

Definition 13.1. Sei R ein Integritätsbereich.

1. Ein Element $d \in R$ heißt Teiler von $a \in R$, wenn gilt $a = dc$ für ein $c \in R$. Wir schreiben in diesem Fall $d|a$.

2. Ein Element $d \in R$ heißt größter gemeinsamer Teiler von $a, b \in R$, wenn $d|a$, $d|b$ und für jedes $d' \in R$ mit $d'|a$, $d'|b$ gilt $d'|d$.

   Der größte gemeinsame Teiler ist bis auf Multiplikation mit einem invertierbaren Element definiert (Übungsblatt). Wir bezeichnen einen größten gemeinsamen Teiler von a und b mit $gcd(a, b)$.

Lemma 13.2. *Sei R ein Hauptidealbereich. Dann $gcd(a, b)$ existiert für beliebige $a, b \in R$.*

Beweis. Betrachten wir das Ideal $I = (a, b)$. Da R ein Hauptidealring ist, gilt $I = (d)$ für ein $d \in R$. Zeigen wir, dass $d = gcd(a, b)$:

$$a \in I = (d) \Rightarrow d|a \qquad \text{und} \qquad b \in I = (d) \Rightarrow d|b.$$

Also ist d ein Teiler von a und b.

Sei $d' \in R$ ein weiterer Teiler von a und b, d.h. $d'|a$, $d'|b$. Da d in $I = (a, b)$ enthalten ist, gibt es $a, b \in R$, so dass gilt $d = ax + by$. Daraus folgt $d'|d$. □

Bemerkung 13.3. Sei R ein Hauptidealbereich. Aus dem Beweis des obigen Lemmas folgt: wenn $d = gcd(a, b)$, dann es existieren $x, y \in R$, sodass $d = ax + by$.

Definition 13.4. Ein Ring R heißt

1. noethersch $\iff$ jede aufsteigende Kette von Idealen wird stationär.

2. artinsch $\iff$ jede absteigende Kette von Idealen wird stationär.

Beispiel 13.5. Sei $R = \mathbb{Z}$. Dann ist jede aufsteigen Kette von Idealen von der Form

$$(n_1) \subset (n_2) \dots$$

mit $n_i \in \mathbb{Z}$ und $n_{i+1}|n_i$. Da so ein n_i nur endlich viele Teiler hat, wir die Kette stationär. Also ist $\mathbb{Z}$ noethersch. Aber nicht artinsch: $(2) \supset (4) \supset (8) \dots$.

Lemma 13.6. *Hauptidealringe sind noethersch.*

Beweis. Sei $I_1 \subset I_2 \subset \dots$ eine aufsteigende Kette von Idealen. Betrachten wir das Ideal $I = \cup_{n=1}^{\infty} I_n$. Da I ein Ideal ist, gilt $I = (a)$ mit $a \in R$. Aus $a \in I$ folgt $\exists n : a \in I_n$. Aus $a \in I_n$ folgt $I \subset I_n$. Also gilt $I_k = I_n$ für $k \geq n$. □

Teil 4. Faktorielle Ringe

Definition 13.7. Sei R ein kommutativer Ring.

1. Ein Element $u \in R$ heißt Einheit $\iff$ u hat ein multiplikatives Inverses (d.h. $\exists v \in R$ sodass $uv = 1$).

   Die Einheiten in R bilden eine Gruppe, die Einheitengruppe, bezüglich der Multiplikation in R. Diese Gruppe bezeichnet man mit R^*

2. Ein Element $a \in R$ heißt irreduzibel $\iff$ $a \notin R^*$ und $a = bc$ impliziert, dass $b \in R^*$ oder $c \in R^*$.

Beispiel 13.8. Sei $R = \mathbb{Z}$. Es gilt

1. $\mathbb{Z}^* = \{-1, 1\}$
2. $n \in \mathbb{Z}$ ist irreduzibel $\iff$ $n = \pm p$ mit p prim.

Sei R ein beliebiger kommutativer Ring, $a \in R$ und $u \in R^*$. Es ist sofort klar, dass folgendes gilt $(a) = (au)$. Wenn R zusätzlich ein Integritätsbereich ist, dann gilt auch die Umkehrung.

Lemma 13.9. *Sei R ein Integritätsbereich und $a, b \in R$. Dann gilt*

$$(a) = (b) \iff b = ua \text{ mit } u \in R^*.$$

Beweis. $\Rightarrow$) OBDA $b \neq 0$. Dann gilt:

$$(a) = (b) \Rightarrow b \in (a) \Rightarrow b = xa \text{ mit } x \in R$$
$$(a) = (b) \Rightarrow a \in (b) \Rightarrow a = yb \text{ mit } y \in R$$

Daraus folgt $bxy = b$. Wir haben

$$bxy = b \iff b(xy - 1) = 0 \iff xy - 1 \Rightarrow x \in R^*.$$

□

Lemma 13.10. *Sei R ein Hauptidealbereich, $p \in R$ ein irreduzibles Element und $p|ab$. Dann gilt: $p|a$ oder $p|b$.*

Beweis. Wenn gilt $p|a$, dann sind wir fertig. Also nehmen wir an, dass gilt $p \nmid a$ und zeigen, dass gilt $p|b$. Wir haben

$$p \nmid a \Rightarrow \exists x, y \in R, \text{ sodass } px + ay = 1 \Rightarrow bpx + bay = b.$$

Da p die linke Seite $bpx + bay$ teilt, muss p auch die rechte Seite b teilen. □

Lemma 13.11. *Sei R ein Integritätsbereich und $a \in R$. Ist das Ideal $(a) \subset R$ prim, dann ist a irreduzibel.*

Beweis. Sei $a = bc$ eine Faktorisierung von a. Da (a) ein Primideal ist, ist entweder b oder c in (a) enthalten, etwa b. Dann haben wir

$$b \in (a) \Rightarrow b = ax = bcx \Rightarrow 1 = cx.$$

Dann ist c invertierbar. □

Definition 13.12.

1. Ein Element $a \neq 0 \in R$ besitzt eine eindeutige Zerlegung in irreduzible Faktoren, wenn gilt $a = u \prod_{i=1}^{n} p_i$ mit $u \in R^*$ und p_i irreduzibel, und außerdem für jede solche Darstellung $a = u' \prod_{i=1}^{m} p'_i$ gilt: $m = n$ und $p_i = v_i p'_i$ mit $v_i \in R^*$.

2. Ein Ring R heißt faktoriell $\iff$ Integritätsbereich + jedes Element besitzt eine eindeutige Zerlegung in irreduzible Faktoren.

Beispiel 13.13.

1. $\mathbb{Z}$ ist faktoriell.

2. $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell:

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

   Die Elemente $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ sind irreduzibel in $\mathbb{Z}[\sqrt{-5}]$ (Übungsblatt 9).

14 30.05.18 — Ringe VI

Teil 4. fortgesetzt

Definition 14.1. Sei R ein kommutativer Ring.

1. $u \in R$ heißt Einheit $\iff$ u hat ein multiplikatives Inverses.
2. $a \in R$ heißt irreduzibel $\iff$ $a \notin R^*$ und $a = bc$ impliziert, dass $b \in R^*$ oder $c \in R^*$.
3. $x \in R$ heißt prim $\iff$ das Ideal (x) ist ein Primideal.[4]

Bemerkung 14.2. In einem Integritätsbereicht ist jedes Primlement irreduziebel (Lemma 13.11). Die Umkehrung ist im Allgemeinem falsch (e.g. in $\mathbb{Z}[\sqrt{-5}]$, siehe Übungsblatt 9).

Lemma 14.3. *Sei R ein Integritätsbereich. Für ein Element $a \in R$ habe man Zerlegungen*

$$a = p_1 \dots p_r = q_1 \dots q_s$$

in Primelemente p_i und irreduzible Elemente q_j. Dann gilt $r = s$, und nach eventueller Umnummerierung der q_j ist p_i assoziiert zu q_i für $i = 1, \dots, r$.

Beweis. Aus $p_1 | q_1 \dots q_s$ folgt, dass es ein j mit $p_1 | q_j$ gibt. Nach Umnummerierung der q_j dürfen wir $j = 1$ annehmen. Aus $p_1 | q_1$ folgt $q_1 = p_1 u$ mit $u \in R^*$. Somit folgt

$$p_2 \dots p_r = u q_2 \dots q_s,$$

und man kann induktiv fortsetzen. □

Satz 14.4. *Sei R ein Integritätsbereich. Dann ist äquivalent:*

1. *Jedes $a \in R \setminus (R^* \cup \{0\})$ lässt sich eindeutig (bis auf Assoziiertheit und Reihenfolge) als Produkt von irreduziblen Elementen schreiben.*
2. *Jedes $a \in R \setminus (R^* \cup \{0\})$ lässt sich eindeutig (bis auf Assoziiertheit und Reihenfolge) als Produkt von Primelementen schreiben.*

Beweis. 1. $\Rightarrow$ 2.) Es genügt zu zeigen, dass jedes irreduzible Element schon prim ist. Sei $q \in R$ irreduzibel, und seien $x, y \in R$ mit $q | xy$. Zerlegen wir die Elemente $x, y \in R$ in Irreduzible: $x = x_1 \dots x_n$ und $y = y_1 \dots y_m$. Dann folgt $q | x_1 \dots x_n y_1 \dots y_m$, und die Eindeutigkeit der Zerlegung impliziert, dass q zu einem x_i oder einem y_j assziiert ist. Daher gilt $q | x$ oder $q | y$, und q ist ein Primelement. Die Eindeutigkeit dieser Zerlegung (bis auf Assoziiertheit und Reihenfolge) folgt jetzt nach Lemma 14.3.

2. $\Rightarrow$ 1.) Nach Lemma 13.11 ist jedes Primelement irreduzibel. Dann implizieren die Voraussetzungen der Aussage 2, dass jedes Element $a \in R \setminus (R^* \cup \{0\})$ sich als Produkt von irreduziblen schreiben lässt. Die Eindeutigkeit dieser Zerlegung (bis auf Assoziiertheit und Reihenfolge) folgt jetzt nach Lemma 14.3.

□

[4] Äquivalent kann man sagen $x | ab$ impliziert $x | a$ oder $x | b$.

Definition 14.5. Ein Integritätsbereich R heißt faktoriell, wenn die äquivalenten Bedingungen des Lemmas erfüllt sind.

Bemerkung 14.6. In einem faktoriellen Ring ist ein Element a genau dann irreduzibel, wenn es prim ist.

Theorem 14.7. *Sei R ein Hautidealbereich. Dann ist R faktorieller Ring.*

Beweis. Sei $a \in R \setminus (R^* \cup \{0\})$.

1. a hat einen irreduziblen Teiler:

   Falls a irreduzibel ist, ist die Aussage klar. Also wir nehmen an, dass a reduzibel ist, d.h. $a = a_1 x$ mit Nichteinheiten $a_1, x \in R$. Falls a_1 irreduzibel ist, sind wir fertig. Falls nicht, dann a_1 in Nichteinheiten faktorisiren. Wiederholen.

   Auf diese Weise erhalten wir eine aufsteigende Kette von Idealen

   $$(a) \subset (a_1) \subset (a_2) \subset \dots.$$

   Da jeder Hauptidealring noethersch ist, wird diese Kette stationär. Daraus folgt, dass es ein N existiert, sodass $(a_i) = (a_N)$ für $i \geq N$. Dann ist a_N irreduzibel.

2. a lässt sich als Produkt von irreduziblen Elementen schreiben:

   Sei q_1 ein irreduzibler Teiler von a (er existiert nach Schritt 1). Dann können wir a schreiben als $a = q_1 b_1$. Dann dasselbe mit b_1 wiederholen

   $$a = q_1 q_2 b_2$$

   und so weiter. Auf diese Weise erhalten wir entweder eine Zerlegung in irreduzible Faktoren

   $$a = q_1 q_2 \dots q_n,$$

   oder eine aufsteigende Kette von Idealen

   $$(a) \subset (q_1) \subset (q_2) \subset \dots,$$

   die nicht stationär wird. Da R noethersch ist, ist die zweite Möglichkeit ausgeschlossen.

3. Eindeutigkeit folgt aus Lemma 13.10 und Lemma 14.3.

□

Korollar 14.8. *$\mathbb{Z}$ und $K[x]$ sind faktoriell.*

Es gibt faktorielle Ringe, die keine Hauptidealbereiche sind (z.B. $\mathbb{Z}[x]$ oder $K[x, y]$). Unser nächstes Ziel ist das folgende Resultat.

Theorem 14.9 (Satz von Gauß)**.** *Sei R ein faktorieller Ring. Dann ist auch der Polynomring in einer Variable $R[x]$ faktoriell.*

Um dieses Theorem zu beweisen, brauchen wir noch einige Vorbereitungen. Aber wir können schon jetzt eine Folgerung formulieren.

Korollar 14.10. *Ist R ein faktorieller Ring, so ist der Polynomring $R[x_1, \ldots, x_n]$ faktoriell. Insbesondere, ist K ein Körper, so ist der Polynomring $K[x_1, \ldots, x_n]$ faktoriell.*

Definition 14.11. Sei R ein Integritätsbereich. Betrachten wir die Menge aller Paare

$$M = \{(a, b) \mid a \in R, b \in R \setminus \{0\}\}.$$

Auf M führen wir eine Äquivalenzrelation $\sim$ ein,[5] indem wir setzen

$$(a, b) \sim (a', b') \iff ab' = ba'.$$

Es sei

$$Q(R) = M/\sim$$

die Menge der Äquivalenzklassen. Für $(a, b) \in M$ bezeichnen wir mit $\frac{a}{b}$ die zugehörige Äquivalenzklasse, so dass gilt

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = ba'.$$

Es ist nicht schwer zu zeigen, dass $Q(R)$ mit der gewönlichen Addition und Multiplikation von Brüchen

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

ein Körper ist.[6] Der Ring $Q(R)$ wird Quotientenkörper von R genannt. Die natürliche Abbildung

$$\begin{aligned} R &\to Q(R) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

ist ein injektiver Ringhomomorphismus.[7] Man kann also R als Unterring vom Körper $Q(R)$ betrachten.

Beispiel 14.12.

1. $Q(\mathbb{Z}) = \mathbb{Q}$.
2. $Q(K[x]) = K(x)$.

[5] Übung: Zeigen Sie, dass $\sim$ ein Äquivalenzrelation ist.
[6] Übung: Zeigen Sie, dass die Addition und Multiplikation wohldefiniert sind und $Q(R)$ ein Körper ist.
[7] Übung: Beweisen Sie diese Aussage.

15 06.06.18 — Ringe VII

Teil 4. fortgesetzt

Definition 15.1. 1. Sei R ein faktorieller Ring und P ein Vertretersystem von Primelementen, d.h. aus jeder Klasse zueinander assoziierter Primelmente enthält P genau eines. Dann lässt sich jedes Element $a \in R \setminus \{0\}$ in der Form

$$a = u \prod_{p \in P} p^{\nu_p(a)} \tag{15.1}$$

schreiben wobei, $u \in R^*$ und $\nu_p(a) \in \mathbb{Z}_{\geq 0}$ eindeutig bestimmt sind. Das Produkt (15.1) ist endlich, d.h. $\nu_p(a) = 0$ für fast alle $p \in P$.

2. Wir betrachten jetzt R als Unterring von $Q(R)$ und erweitern (15.1) darauf. Jedes $\frac{a}{b} \in Q(R)^* = Q(R) \setminus \{0\}$ lässt sich schreiben als

$$\frac{a}{b} = u \prod_{p \in P} p^{\nu_p(\frac{a}{b})},$$

mit $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b) \in \mathbb{Z}$.

3. Für ein Polynom

$$f = \sum_{i=0}^{n} a_i x^i \in Q(R)[x]$$

setzen wir

$$\nu_p(f) := \min_i \nu_p(a_i).$$

Beispiel 15.2. Sei $R = \mathbb{Z}$ und $f = 6x^2 + 4 \in \mathbb{Z}[x]$. Als Vertretersystem von Primelementen nehmen wir positive Primzahlen. Dann gilt

$$\begin{aligned} \nu_2(f) &= 1, \\ \nu_p(f) &= 0\,, \quad p \neq 2. \end{aligned}$$

Bemerkung 15.3.

1. Ein Polynom $f \in Q(R)[x]$ liegt bereits in $R[x]$ genau dann wenn $\nu_p(f) \geq 0$ für alle p.
2. Die oben definierte Abbildung
$$\nu_p \colon Q(R)^* \to \mathbb{Z}$$
ist ein Gruppenhomomorpshimus.

Lemma 15.4 (Gauß)**.** *Es sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für $f, g \in Q(R)[x]$*

$$\nu_p(fg) = \nu_p(f) + \nu_p(g). \tag{15.2}$$

Beweis. (a) Es ist klar, dass (15.2) für konstante Polynome gilt.

(b) Betrachten wir den allgemeinen Fall. OBDA: $f, g \neq 0$, $f, g \in R[x]$ (mit den Nenner multiplizieren), $\nu_p(f) = 0 = \nu_p(g)$ (mit dem GGT der Koeffizienten teilen). Jetzt müssen wir $\nu_p(fg) = 0$ zeigen. Hierzu betrachten wir den Homomorphismus

$$\Phi\colon R[x] \to (R/(p))[x],$$

welcher die Koeffizienten reduziert. Der Kern Ker Φ besteht aus allen denjenigen Polynomen in $R[x]$, deren Koeffizienten sämtlich durch p teilbar sind

$$\text{Ker } \Phi = \{f \in R[x] \mid \nu_p(f) > 0\}.$$

Da $\nu_p(f) = 0 = \nu_p(g)$, gilt $\Phi(f), \Phi(g) \neq 0$. Da $R/(p)$ und $(R/(p))[x]$ Integritätsbereiche sind, folgt

$$\Phi(fg) = \Phi(f)\Phi(g) \neq 0.$$

Also gilt $\nu_p(fg) = 0$. □

Korollar 15.5. *Es sei R ein faktorieller Ring.*

1. *Es sei $h \in R[x]$ ein normiertes*[8] *Polynom und $h = fg$ eine Zerlegung in normierte Polynome $f, g \in Q(R)[x]$. Dann gilt bereits $f, g \in R[x]$.*
2. *Es sei $h \in R[x]$ ein Polynom und $h = fg$ eine Zerlegung mit $f \in R[x]$ primitiv*[9]*. Dann gilt $g \in R[x]$.*

Beweis. Mit dem Lemma von Gauß bekommen wir:

1. $\nu_p(h) = 0, \quad \nu_p(f) \leq 0, \quad \nu_p(g) \leq 0 \quad \Rightarrow \quad \nu_p(f) = \nu_p(g) = 0 \quad \Rightarrow \quad f, g \in R[x].$
2. $\nu_p(h) \geq 0 \quad \text{und} \quad \nu_p(f) = 0 \quad \Rightarrow \quad \nu_p(g) \geq 0 \quad \Rightarrow \quad g \in R[x].$

□

Satz 15.6 (Gauß)**.** *Es sei R ein faktorieller Ring.*

1. *Ein Polynom $q \in R[X]$ der Form*
   - *(a) q ist Primelement in R*
   - *(b) q ist primitiv in $R[x]$ und Primelement in $Q(R)[x]$.*

[8] Ein Polynom heißt normiert, wenn sein Leitkoeffizient gleich 1 ist.
[9] Ein Polynom heißt primitiv, wenn gilt $\gcd(a_i) = 1$.

ist Primelement in $R[x]$.

2. *Alle Primelemente in $R[x]$ sind der Form 1.(a) und 1.(b).*

3. *Der Ring $R[x]$ ist faktoriell.*

Beweis. 1a. Sei q ein Primelement in R. Dann ist $R/(q)$ und somit auch $R[x]/(q) = (R/(q))[x]$ ein Integritätsbereich. Daraus folgt, dass $q \in R[x]$ ein Primelement ist.

1b. Betrachten wir ein primitives Polynom $q \in R[x]$ mit der Eigenschaft, dass q ein Primelement in $Q(R)[x]$ ist. Wir müssen zeigen, dass aus $q|fg$ folgt $q|f$ oder $q|g$.

Nehmen wir an, dass gilt $q|fg$ mit $f, g \in R[x]$. Dann gilt auch $q|fg$ in $Q(R)[x]$. Da q ein Primelement in $Q(R)[x]$ ist, gilt bereits $q|f$ oder $q|g$. Wenn gilt $q|f$, dann haben wir $f = qh$ mit $h \in Q(R)[x]$. Daraus folgt nach Korollar 15.5, dass bereits gilt $h \in R[x]$. Also ist q ein Primelement in $R[x]$.

2.+3. Es genügt zu zeigen, dass jedes Polynom $f \in R[x]$ in ein Produkt von Primelementen der Form gegeben in 1.a und 1.b zerfällt. Jedes $f = \sum_{i=0}^{n} a_i x^i$ kann man als Produkt

$$f = a\tilde{f}$$

schreiben mit $a = gcd(a_i) \in R$ und $\tilde{f}$ primitiv. Sei $\tilde{f} = c\tilde{f}_1 \dots \tilde{f}_r$ eine Zerlegung in Primelemente in $Q(R)[x]$ mit $c \in Q(R)^*$ (es ist bereits bekannt, dass $Q(R)[x]$ faktoriell ist). Nach geeigneter Wahl von c dürfen wir alle $\tilde{f}_i$ als primitiv in $R[x]$ voraussetzen. Dann nach Lemma von Gauß gilt

$$\nu_p(\tilde{f}) = \nu_p(c) + \nu_p(\tilde{f}_1) + \dots + \nu_p(\tilde{f}_r) \quad \Rightarrow \quad \nu_p(c) = 0.$$

Dann ist $\tilde{f} = c\tilde{f}_1 \dots \tilde{f}_r$ die gewünschte Zerlegung in $R[x]$.

□

Teil 5. Irreduzibilitätskriterien

Satz 15.7 (Eisensteinsches Irreduzibilitätskriterium)**.** *Es sei R ein faktorieller Ring und $f = a_n x^n + \dots + a_0 \in R[x]$ ein primitives Polynom vom Grad $n > 0$. Weiter sei $p \in R$ ein Primelement mit*

$$p \nmid a_n, \quad p \mid a_i \text{ für } i < n, \quad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $R[x]$.

Satz 15.8 (Reduktionskriterium)**.** *Es sei R ein faktorieller Ring, $f = a_n x^n + \dots + a_0 \in R[x]$ ein Polynom vom Grad $n > 0$ und $p \in R$ ein Primelement mit $p \nmid a_n$. Weiter sei $\Phi\colon R[x] \to (R/(p))[x]$ der kanonische Homomorphismus, welcher die Koeffizienten reduziert. Dann gilt:*

Ist $\Phi(f)$ irreduzibel in $(R/(p))[x]$, so ist f irreduzibel in $Q(R)[x]$. Ist f zusätzlich primitiv, so ist f irreduzibel in $R[x]$.

16 07.06.18 — Körper I

Teil 1. Die Charakteristik eines Körpers

Definition 16.1. Ein kommutativer Ring K heißt ein Körper, wenn jedes $x \in K \setminus \{0\}$ (bezüglich Multiplikation) invertierbar ist.

Sei K ein Körper. Es ist bekannt, dass es einen eindeutigen Ringhomomorphismus

$$\begin{aligned} \psi \colon \mathbb{Z} &\to K \\ n &\mapsto n \end{aligned}$$

gibt (hier kann man K mit einem beliebigen Ring R ersetzen). Nach dem Homomorphiesatz bekommen wir einen injektiven Ringhomomorpshimus

$$\bar{\psi} \colon \mathbb{Z}/\mathrm{Ker}\ \psi \to K.$$

Da K ein Integritätsbereich ist, muss auch $\mathbb{Z}/\mathrm{Ker}\ \psi$ ein Integritätsbereich sein. Daraus folgt, dass es zwei Alternativen gibt

$$\mathrm{Ker}\ \psi = (0) \tag{16.1}$$
$$\mathrm{Ker}\ \psi = (p) \text{ für eine Primzahl } p \in \mathbb{Z}. \tag{16.2}$$

Definition 16.2. Sei K ein Körper. Im Fall (16.1) sagt man, dass K ein Körper von Charakteristik 0 ist. Im Fall (16.2) sagt man, dass K ein Körper von Charakteristik p ist.

Bemerkung 16.3. Sei K ein Körper von Charakteristik p. Dann ist p die kleinste positive ganze Zahl mit der Eigenschaft

$$\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$$

in K.

Beispiel 16.4.

1. $char(\mathbb{Q}, \mathbb{R}, \mathbb{C}) = 0$.
2. $char(\mathbb{F}_p) = p$.

Lemma 16.5.

1. *Sei K ein Körper und $I \subset K$ ein Ideal. Dann gilt: $I = (0)$ oder $I = K$.*
2. *Jeder Homomorpshismus von Körpern ist injektiv.*

Beweis.

1. Sei $I \subset K$ ein Ideal mit $0 \neq I$ und $0 \neq x \in I$ ein Element. Dann gilt $1 = xx^{-1} \in I$ und somit auch $I = K$.

2. Ein Ringhomomorpshismus $f\colon K_1 \to K_2$ von Körper ist injektiv genau dann, wenn Ker $f = (0)$. Da Kern immer ein echtes Ideal ist (außer $K_2 = \{0\}$, was für ein Körper unmöglich ist), gibt es nur die Möglichkeit Ker $f = (0)$.

□

Bemerkung 16.6. Wenn $F \subset K$, dann gilt $char(F) = char(K)$.

Seien K ein Körper und $F_1, F_2 \subset K$ zwei Unterkörper. Dann ist der Schnitt $F_1 \cap F_2 \subset K$ auch ein Unterkörper. Aus demselben Grund ist der Schnitt aller Unterkörper von K wieder ein Unterkörper von K.

Definition 16.7. Der Schnitt aller Unterkörper heißt Primkörper von K und wird mit P bezeichnet.

Lemma 16.8. *Sei K ein Körper und $P \subset K$ sein Primkörper.*

1. $char(K) = 0 \iff P = \mathbb{Q}$
2. $char(K) = p \iff P = \mathbb{F}_p$

Beweis. $\Leftarrow$) Klar.

$\Rightarrow$) 2. Betrachten wir den natürlichen Homomorphismus $\mathbb{Z} \to P \subset K$. Dann gilt $\mathbb{F}_p \subset P \subset K$. Daraus folgt $\mathbb{F}_p = P$, da P minimal ist.

1. $\mathbb{Z} \to P \subset K$ faktorisiert sich über $\mathbb{Q}$ und wir bekommen $\mathbb{Q} \subset P \subset K$. Daraus folgt $\mathbb{Q} = P$, da P minimal ist.

□

Korollar 16.9. *Sei $\sigma\colon L \to K$ ein Homomorpshimus von Körpern. Dann gilt:*

1. $\mathrm{char}(K) = \mathrm{char}(L)$.
2. *Die Primkörper werden durch σ identifiziert.*

Beweis. Übung. □

Teil 2. Körpererweiterungen

Definition 16.10. Sei $K \subset L$ ein Unterkörper.

1. Man sagt, dass L eine Körpererweiterung von K ist und bezeichnet diese mit L/K.
2. Man kann L als K-Vektorraum betrachten. Die Dimension von L über K wird Grad der Körpererweiterung L/K gennant und mit $[L : K]$ bezeichnet.
3. Eine Körpererweiterung L/K heißt endlich, wenn gilt $[L : K] < \infty$.

Beispiel 16.11.

1. $\mathbb{R} \subset \mathbb{C}$ ist endlich mit $[\mathbb{C} : \mathbb{R}] = 2$.
2. $\mathbb{Q} \subset \mathbb{Q}(t)$ ist nicht endlich.

Lemma 16.12. *Es seien $F \subset K \subset L$ Körpererweiterungen. Dann gilt*

$$[L : F] = [L : K][K : F]. \tag{16.3}$$

Bemerkung 16.13. Die Aussage beinhaltet auch folgendes: L/F ist genau dann endlich, wenn L/K und K/F endlich sind. Also man kann in (16.3) auch ∞ als Dimension einsetzen.

Beweis. Wir betrachten den Fall, dass alle Erweiterungen endlich sind. Der Rest wird dem Leser als Übung überlassen.

Erinnern Sie sich an den Inhalt der 2. Vorlesung. Insbesondere sind Definition 2.6 und Lemma 2.7 für uns relevant. Wenn Sie lineare Algebra schon gehört haben, sollte Folgendes mehr oder weniger offensichtlich für Sie sein.

Sei $x_1, \dots, x_n$ eine Basis von K über F (also gilt $[K : F] = n$), und sei $y_1, \dots, y_m$ eine Basis von L über K (also gilt $[L : K] = m$). Wir werden gleich zeigen, dass $\{x_i y_j\}_{1 \le i \le n, 1 \le j \le m}$ eine Baisis von L über F ist.

Erstens kann man jedes $a \in L$ als Linearkombination von $x_i y_j$ schreiben. Wir haben

$$a = \sum_{i=1}^{m} a_i y_i \qquad \text{mit} \quad a_i \in K$$

$$a_i = \sum_{j=1}^{n} b_{ij} x_j \qquad \text{mit} \quad b_{ij} \in F$$

$$a = \sum_{j=1}^{n} \sum_{i=1}^{m} b_{ij} x_j y_i.$$

Zweitens sind $\{x_i y_j\}_{1 \le i \le n, 1 \le j \le m}$ linear unabhängig über F. Sei

$$\sum_{i,j} c_{ij} x_j y_i = 0.$$

eine lineare Relation. Daraus bekommen wir eine lineare Relation zwischen y_i's

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{m} c_{ij} x_j \Big) y_i = 0.$$

Da diese aber linear unabhängig sind, bekommen wir, dass gilt

$$\sum_{i=1}^{m} c_{ij} x_j = 0 \qquad \forall j.$$

Da die x_i auch linear unabhängig sind, gilt

$$c_{ij} = 0 \qquad \forall i, j$$

□

17 13.06.18 — Körper II

Teil 2. fortgesetzt

Definition 17.1. Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt algebraisch über K, wenn es ein Polynom $0 \neq f(x) \in K[x]$ gibt, sodass gilt $f(\alpha) = 0$. Ansonsten sagt man, dass α transzendent über K ist. Mann nennt L/K algebraisch, wenn jedes $\alpha \in L$ algebraisch über K ist.

Beispiel 17.2.

1. Betrachten wir die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$. Das Element $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, weil es eine Lösung der Gleichung $x^2 + 1 = 0$ ist.
2. $\mathbb{Q} \subset \mathbb{R}$, das Element $\alpha = \sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, aber $\pi \in \mathbb{R}$ ist transzendent.

Lemma 17.3. *Jede endliche Körpererweiterung L/K ist algebraisch.*

Beweis. Sei $\alpha \in L$. Da $\dim_K L < \infty$, gibt es ein $n \in \mathbb{Z}$, sodass die Elemente $1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig sind. D.h. es gibt $a_0, \ldots, a_n$, sodass $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Dann gilt $f(\alpha) = 0$ mit $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. □

Definition 17.4. Sei L/K eine Körpererweiterung und $\alpha \in L$ ein Element. Betrachten wir den Homomorphismus

$$\begin{aligned} \psi_\alpha \colon K[x] &\to L \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

Das Bild von ψ_α wird mit $K[\alpha]$ bezeichnet.

Da L ein Intergritätsbereich ist, ist auch $K[\alpha]$ ein Intergritätsbereich. Den Quotientenkörper von $K[\alpha]$ bezeichnen wir mit $K(\alpha)$.

Es ist α genau dann algebraisch über K, wenn ψ_α nicht injektiv ist. Da $K[x]$ ein Hauptidealbereich ist, gilt

$$\operatorname{Ker} \psi_\alpha = (p(x)),$$

wobei $p(x)$ ein irreduzibles Polynom ist. Hier kann man $p(x)$ normiert voraussetzen (d.h. Leitkoeffizient = 1). Dieses Polynom ist eindeutig definiert und wird Minimalpolynom von α über K genannt.

Lemma 17.5. *Seien L/K eine Körpererweiterung, $\alpha \in L$ ein Element, das algebraisch über K ist, und $p(x) \in K[x]$ das Minimalpolynom von α. Dann gilt:*

1. $K[\alpha] = K(\alpha)$.
2. $[K(\alpha) : K] = \deg p(x)$.

Beweis. 1. Betrachten wir ein Element $0 \neq \beta \in K[\alpha]$. Dann gilt $\beta = f(\alpha)$ für ein $f(x) \in K[x]$. Dann gilt $(p(x), f(x)) = K[x]$, da das Ideal $(p(x))$ maximal ist und $f(x)$ nicht in $(p(x))$ liegt. Es existieren Polynome $a(x), b(x) \in K[x]$, sodass gilt

$$a(x)p(x) + b(x)f(x) = 1. \qquad (*)$$

Wenn wir jetzt α anstatt von x in $(*)$ einsetzen, bekommen wir $b(\alpha)f(\alpha) = 1$. Also ist $\beta = f(\alpha)$ invertierbar, und somit ist $K[\alpha]$ ein Körper.

2. Sei $n = \deg p(x)$. Aus der Definition von $p(x)$ folgt es sofort, dass $1, \alpha, \alpha^2, \dots \alpha^{n-1}$ eine Basis von $K[\alpha]$ über K ist.

□

Definition 17.6. Sei L/K eine Körpererweiterung und $\alpha_1, \dots, \alpha_n \in L$ beliebige Elemente. Betrachten wir den natürlichen Homomorphismus

$$\begin{aligned} \psi_\alpha \colon K[x_1, \dots, x_n] &\to L \\ f(x_1, \dots, x_n) &\mapsto f(\alpha_1, \dots, \alpha_n) \end{aligned}$$

Das Bild von ψ_α wird mit $K[\alpha_1, \dots, \alpha_n]$ bezeichnet, und ist ein Intergritätsbereich. Sein Quotientenkörper bezeichnen wir mit $K(\alpha_1, \dots, \alpha_n)$.

Eine Körpererweiterung L/K heißt endlich erzeugt, wenn es Elemente $\alpha_1, \dots, \alpha_n \in L$ gibt, sodass gilt $L = K(\alpha_1, \dots, \alpha_n)$.

Lemma 17.7. *Sei $L = K(\alpha_1, \dots, \alpha_n)$, wobei alle α_i algebraisch über K sind. Dann ist L/K eine endliche Körpererweiterung.*

Beweis. Betrachten wir den Fall $n = 1$, d.h. $K \subset L = K(\alpha)$. Die Aussage folgt hierfür aus Lemma 17.5. Der allgemeine Fall lassen wir als eine kleine Übung. □

Theorem 17.8. *Seien $F \subset K \subset L$ Körpererweiterungen. Dann ist L/F genau dann algebraisch, wenn L/K und K/F algebraisch sind.*

Beweis. $\Rightarrow$) Klar.

$\Leftarrow$) Sei $\alpha \in L$ und $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in K[x]$ sein Minimalpolynom. Betrachten wir den Körper $K' = F(a_0, \dots, a_{n-1})$. Dann haben wir Inklusionen $F \subset K' \subset K'(\alpha)$. Nach Lemma 17.5 ist die Körpererweiterung $K'(\alpha)/K'$ endlich. Da $a_0, \dots, a_{n-1}$ algebraisch über F sind, ist nach Lemma 17.7 die Körpererweiterung $K' = F(a_0, \dots, a_{n-1})/F$ auch endlich. Dann ist nach Lemma 16.12 auch $K'(\alpha)/F$ endlich, und somit ist α algebraisch über F nach Lemma 17.3. □

Korollar 17.9. *Sei L/K eine Körpererweiterung. Dann ist*

$$L_{alg} = \{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$$

ein Unterkörper von L.

Beweis. Seien $\alpha, \beta \in L$ algebraische Elemente. Dann ist der Körper $K(\alpha, \beta)$ endlich über K (Lemma 17.7). Da die Elemente $\alpha + \beta$, $\alpha\beta$, α^{-1} in $K(\alpha, \beta)$ sind, sind diese auch algebraisch über K (Lemma 17.3). □

18 14.06.18 — Körper III

Teil 3. Algebraischer Abschluss eines Körpers

Lemma 18.1. *Sei $f(x) \in K[x]$ ein Polynom über einem Körper K. Es existiert eine endliche Körpererweiterung L/K, so dass $f(x)$ in L eine Nullstelle hat.*

Beweis. Sei $p(x)$ einer der irreduziblen Faktoren von $f(x)$ (Erinnerung: $K[x]$ ist ein faktorieller Ring).

Man betrachte den Faktorring $L = K[y]/(p(y))$. Da $p(y)$ irreduzibel ist, ist $(p(y))$ ein maximales Ideal und somit ist L ein Körper. Da die natürliche Abbildung

$$\begin{aligned} K &\to L = K[y]/(p(y)) \\ a &\mapsto a \end{aligned}$$

injektiv ist, können wir L als eine Körpererweiterung von K betrachten. Es folgt sofort, dass die Klasse α von y in $K[y]/(p(y))$ folgende Eigenschaft hat

$$p(\alpha) = 0.$$

Somit ist α eine Nullstelle von $p(x)$ in L. □

Beispiel 18.2. Das Polynom $x^2 + 1$ hat keine Nullstellen in $\mathbb{R}$. Andererseits hat dieses Polynom im Körper $\mathbb{R}[x]/(x^2 + 1) = \mathbb{C}$ zwei Nullstellen $\pm\bar{x}$.

Korollar 18.3. *Seien $f_1(x), \ldots, f_n(x) \in K[x]$ Polynome. Es existiert eine endliche Körpererweiterung L/K, in welchem jedes $f_i(x)$ eine Nullstelle hat.*

Beweis. Übung. □

Definition 18.4. Ein Körper K heißt algebraisch abgeschlossen, wenn jedes Polynom $f(x) \in K[x]$ eine Nullstelle in K hat.

Bemerkung 18.5. Äquivalent kann man die obige Definition auf folgende Weise umformulieren: Ein Körper K heißt algebraisch abgeschlossen, wenn jedes normierte Polynom $f(x) \in K[x]$ sich als Produkt von linearen Faktoren $f(x) = (x - a_1)(x - a_2)\ldots(x - a_n)$ mit $a_i \in K$ schreiben lässt.

Beispiel 18.6.

1. Der Körper $K = \mathbb{R}$ ist nicht algebraisch abgeschlossen, da das Polynom $x^2 + 1 \in \mathbb{R}[x]$ keine Wurzel in $\mathbb{R}$ hat.

2. Der Körper $K = \mathbb{C}$ ist algebraisch abgeschlossen (ohne Beweis).

Theorem 18.7. *Jeder Körper K lässt sich in einen algebraisch abgeschlossenen Körper einbetten. D.h. es existiert ein algebraisch abgeschlossener Körper L und ein Monomorphismus $K \to L$.*

Beweis. Der Beweis hat drei Schritte.

1. Hier konstruieren wir eine Körpererweiterung K_1/K, so dass jedes $f(x) \in K[x]$ eine Nullstelle hat.

   Jedem $f(x) \in K[x]$ ordnen wir eine Variable y_f zu, und betrachten den Polynomring in unendlich vielen Variablen $A := K[y_f]_{f \in K[x]}$. Sei $I \subset A$ das von allen $f(y_f) \in A$ erzeugte Ideal.

   Das Ideal $I \subset A$ ist ein echtes Ideal. Nehmen wir das Gegenteil an. Dann gibt es Elemente $g_1, \ldots, g_n \in A$ und $f_1, \ldots, f_n \in K[x]$, sodass gilt

   $$g_1 f_1(y_{f_1}) + \cdots + g_n f_n(y_{f_n}) = 1. \qquad (*)$$

   Da $g_1, \ldots, g_n$ nur endlich viele Variablen enthalten, gibt es ein $N \in \mathbb{Z}$, sodass $(*)$ als Gleichung in $A' = K[y_{f_1}, \ldots, y_{f_n}, \ldots, y_{f_N}]$ betrachtet werden kann. Sei L eine Körpererweiterung von K, in welchem f_i für $0 \leq i \leq n$ eine Nullstelle haben (Lemma 18.3). Bezeichnen wir diese Nullstellen mit α_i für $0 \leq i \leq n$ und setzen weiter zusätzlich $\alpha_i = 0$ für $i > n$. Jetzt betrachten wir den Homomorphismus

   $$\begin{aligned} \psi_\alpha \colon A' &\to L \\ y_{f_i} &\mapsto \alpha_i \end{aligned}$$

   und wenden ihn auf $(*)$ an. Dann bekommen wir $0 = 1$. Widerspruch! Also gilt $I \neq A$.

2. Betrachten wir ein maximales Ideal $\mathfrak{m} \subset A$ mit der Eigenschaft $I \subset \mathfrak{m} \subset A$. Da $\mathfrak{m} \subset A$ maximal ist, ist $K_1 := A/\mathfrak{m}$ ein Körper mit $K \subset K_1$. Weiter hat jedes Polynom aus $K[x]$ eine Nullstelle in K_1 (gegeben durch $\overline{y_f}$).

   Wenn wir die Konstruktion aus Schritt 1 wiederholen, bekommen wir eine Kette von Körpererweiterungen

   $$K \subset K_1 \subset K_2 \cdots \subset K_n \subset \ldots$$

   mit der folgenden Eigenschaft: jedes $f(x) \in K_i[x]$ hat eine Nullstelle in K_{i+1}.

   Jetzt betrachten wir die Vereinigung

   $$L := \bigcup_{i=1}^{\infty} K_i.$$

   Es ist leicht zu sehen, dass L ein Körper ist. Zum Beispiel, seien $x, y \in L$. Dann sind x, y schon in einem K_i enthalten. Somit liegen auch $x + y$ und xy bereits in $K_i \subset L$.

3. Sei $f(x) \in L[x]$. Da $f(x)$ nur endlich vielen Koeffizienten hat, liegt es bereit in einem $K_i[x]$. Somit hat $f(x)$ eine Nullstelle in $K_{i+1} \subset L$.

□

Korollar 18.8. *Für jeden Körper K existiert ein algebraisch abgeschlossener Körper $\overline{K}$, sodass die Körpererweiterung $\overline{K}/K$ algebraisch ist.*

Beweis. Nach Theorem 18.7 können wir K in einen algebraisch abgeschlossenen Körper L einbetten. Jetzt setzen wir $\overline{K} = L_{alg}$, welcher nach Korollar 17.9 ein Unterkörper von L und algebraisch über K ist.

Jetzt zeigen wir, dass $\overline{K}$ algebraisch abgeschlossen ist. Sei $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \overline{K}[x]$ ein Polynom. Da L algebraisch abgeschlossen ist, hat $f(x)$ eine Nullstelle α in L. Betrachten wir jetzt die Körpererweiterungen

$$K \subset K(a_0, \ldots, a_n) \subset K(a_0, \ldots, a_n)(\alpha).$$

Da alle a_i algebraisch über K sind, ist die Körpererweiterung $K \subset K(a_0, \ldots, a_n)$ algebraisch (Lemma 17.7). Die Körpererweiterung $K(a_0, \ldots, a_n) \subset K(a_0, \ldots, a_n)(\alpha)$ ist algebraisch nach Konstruktion. Dann ist auch die Körpererweiterung $K \subset K(a_0, \ldots, a_n)(\alpha)$ algebraisch (Theorem 17.8). Daraus folgt, dass α algebraisch über K ist, und liegt somit in $\overline{K}$. □

Definition 18.9. Der Körper $\overline{K}$ aus Korollar 18.8 heißt algebraischer Abschluss von K.

Bemerkung 18.10. Später werden wir sehen, dass alle algebraische Abschlüsse eines Körpers K isomorph sind.

Beispiel 18.11. $\overline{\mathbb{R}} = \mathbb{C}$.

19 20.06.18 — Körper IV

Teil 4. Fortsetzung von Homomorphismen

Notation 19.1. Sei $\sigma\colon K \to L$ ein Homomorphismus von Körpern. Wir schreiben

$$a^\sigma := \sigma(a)$$

für $a \in K$ und

$$f^\sigma(x) := \sum_i a_i^\sigma x^i$$

für ein Polynom $f(x) = \sum_i a_i x^i$.

Definition 19.2. Seien K'/K und L'/L Körpererweiterungen, und seien $\sigma\colon K \to L$ und $\tau\colon K' \to L'$ Homomorphismen. Man sagt, dass τ eine Fortsetzung von σ ist, wenn gilt $\tau_{|K} = \sigma$. Mit anderen Worten ist τ eine Fortsetzung von σ, wenn das Diagramm

$$\begin{array}{ccc} K' & \xrightarrow{\tau} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & L \end{array}$$

kommutativ ist, wobei die vertikale Pfeile die natürliche Inklusionen $K \subset K'$ und $L \subset L'$ sind.

Lemma 19.3. *Sei $\sigma\colon K \to L$ ein Homomorphismus von Körpern, und seien K'/K und L'/L Körpererweiterungen. Wenn gilt $K' = K(\alpha)$ mit α algebraisch über K, dann ist die Menge von Homomorphismen $\tau\colon K' \to L'$, die σ fortsetzen, in Bijektion mit der Menge von Nullstellen vom Polynom $p^\sigma(x)$ in L', wobei $p(x) \in K[x]$ das Minimalpolynom von α ist.*

Beweis. Sei τ eine solche Fortsetzung. Dann gilt $p^\sigma(\alpha^\tau) = p^\tau(\alpha^\tau) = (p(\alpha))^\tau = 0$. Also ist $\beta = \alpha^\tau \in L'$ eine Wurzel von $p^\sigma(x)$ in L'.

Umgekehrt: Sei $\beta \in L'$ eine Wurzel von $p^\sigma(x)$. Nach Lemma 17.5 kann jedes Element von $K(\alpha)$ als $f(\alpha)$ mit $f(x) \in K[x]$ geschrieben werden. Definieren wir

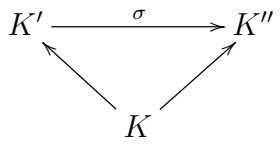
$$(f(\alpha))^\tau := f^\sigma(\beta).$$

Diese Abbildung ist wohldefiniert: Wenn gilt $f(\alpha) = g(\alpha)$, dann gilt $(f-g)(\alpha) = 0$. Daraus folgt $f(x) - g(x) = h(x)p(x)$ mit $h(x) \in K[x]$, und somit gilt auch $f^\sigma(\beta) - g^\sigma(\beta) = h^\sigma(\beta)p^\sigma(\beta) = 0$.

Es ist leicht zu sehen, dass τ ein Homomorphismus ist, und σ fortsetzt. □

Korollar 19.4. *Die Anzahl von möglichen Fortsetzungen von $\sigma\colon K \to L$ auf $K' = K(\alpha)$ ist nicht größer als $[K(\alpha) : K] = \deg p(x)$.*

Definition 19.5. Seien K'/K und K''/K Körpererweiterungen. Man sagt, dass $\sigma\colon K' \to K''$ ein Homomorphismus über K ist, wenn er eine Fortsetzung der Identität $K \to K$ ist. Mit anderen Worten ist σ ein Homomorphismus über K, wenn das Diagramm



kommutativ ist, wobei die vertikale Pfeile die natürliche Inklusionen $K \subset K'$ und $K \subset K''$ sind.

Lemma 19.6. *Seien L/K eine algebraische Körpererweiterung und $\sigma\colon L \to L$ ein K-Homomorphismus. Dann ist σ ein Automorphismus.*

Beweis. Da L ein Körper ist, genügt es, die Surjektivität zu zeigen. Seien $\alpha \in L$, $p(x)$ sein Minimalpolynom, $\alpha_1, \dots, \alpha_m$ alle Wurzeln von $p(x)$ in L und $L' = K(\alpha_1, \dots, \alpha_m)$. Da $\alpha_1, \dots, \alpha_m$ algebraisch über K sind, ist L'/K endlich (Lemma 17.7). Es ist klar, dass gilt $\sigma(\alpha_i) = \alpha_j$. Dann bekommen wir durch Einschränken den Homomorphismus $\sigma_{|L'}\colon L' \to L'$. Da $\sigma_{|L'}$ injektiv und K-linear ist, ist er automatisch surjektiv, da L'/K eine endliche Erweiterung ist (analog zu endlichen Mengen). Also liegt α im Bild von σ. □

Theorem 19.7. *Sei K'/K eine algebraische Körpererweiterung und $\sigma\colon K \to L$ ein Homomorphismus mit L algebraisch abgeschlossen. Dann existiert ein Homomorphismus $\sigma'\colon K' \to L$, der σ fortsetzt.*

Beweis. Sei $K'' \subset K'$ ein maximaler Körper (Lemma von Zorn), auf welchen σ sich fortsetzen lässt (diese Fortsetzung bezeichnen wir mit σ''), und nehmen wir an, dass gilt $K'' \neq K'$. Sei $\alpha \in K'' \setminus K$. Dann können wir nach Lemma 19.3 σ'' auf $K''(\alpha)$ fortsetzen. Widerspruch. □

Korollar 19.8. *Seien $\overline{K}'/K$ und $\overline{K}''/K$ zwei algebraische Abschlüsse von K. Dann sind $\overline{K}'$ und $\overline{K}''$ isomorph über K. Genauer ist sogar jeder K-Homomorpshismus $\overline{K}' \to \overline{K}''$ ein Isomorphismus.*

Beweis. Nach Theorem 19.7 bekommen wir Homomorphismen $\sigma\colon \overline{K}' \to \overline{K}''$ und $\tau\colon \overline{K}'' \to \overline{K}'$. Nach Lemma 19.6 sind $\sigma \circ \tau$ und $\tau \circ \sigma$ Automorphismen. Daraus folgt, dass σ und τ Isomorphismen sind. □

20 21.06.18 — Körper V

Teil 5. Zerfällungskörper

Sei K ein Körper und $f(x) \in K[x]$ ein Polynom.

Definition 20.1. Ein Körper $L \supset K$ heißt Zerfällungskörper von $f(x)$, wenn $f(x)$ sich in $L[x]$ als Produkt von Linearfaktoren $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$ schreiben lässt, und es gilt $L = K(\alpha_1, \dots, \alpha_n)$.

Beispiel 20.2.

1. Der Körper $\mathbb{C}$ ist der Zerfällungskörper von $x^2 + 1 \in \mathbb{R}[x]$.
2. Der Körper $\mathbb{Q}(\sqrt[3]{2})$ ist kein Zerfällungskörper für $x^3 - 2$.

Lemma 20.3.

1. *Jeder algebraischer Abschluss $\overline{K}$ von K enthält einen eindeutigen Körper L, welcher der Zerfällungskörper von $f(x)$ ist.*
2. *Jede Einbettung über K $\sigma\colon L \to \overline{K}$ ist ein Automorphismus von L.*
3. *Je zwei Zerfällungskörper von $f(x)$ sind isomorph.*

Beweis.

1. Da $\overline{K}$ algebraisch abgeschlossen ist, gilt $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$ mit $c \in K$ und $\alpha_i \in \overline{K}$. Dann setzen wir $L = K(\alpha_1, \dots, \alpha_n)$. Keine andere Wahl laut Definition.
2. Da σ die Nullstellen von $f(x)$ auf die Nullstellen von $f(x)$ abbildet, wird dadurch ein Homomorphismus $L \to L$ induziert, welcher dann automatisch ein Automorphismus ist (Lemma 19.6).
3. Übung.

□

Definition 20.4. Sei $\{f_i(x)\}_{i\in I}$ eine Familie von Polynomen in $K[x]$. Der Zerfällungskörper von $\{f_i(x)\}_{i\in I}$ ist ein Körper $L \supset K$, sodass alle $f_i(x)$ sich über L als Produkt von Linearfaktoren schreiben lassen, und L durch alle Nullstellen von $f_i(x)$ erzeugt wird.

Lemma 20.5.

1. *Jeder algebraischer Abschluss $\overline{K}$ von K enthält einen eindeutigen Körper L, welcher der Zerfällungskörper der Familie von Polynomen $\{f_i(x)\}_{i\in I}$ ist.*
2. *Jede Einbettung über K $\sigma\colon L \to \overline{K}$ ist ein Automorphismus von L.*
3. *Je zwei Zerfällungskörper von $\{f_i(x)\}_{i\in I}$ sind isomorph.*

Beweis. Ähnlich zu Lemma 19.11. Übung. □

Teil 6. Normale Körpererweiterungen

Definition 20.6. Sei L/K eine algebraische Körpererweiterung, $L \subset \overline{K}$. Die Körpererweiterung L/K heißt normal, wenn jeder Homomorphismus $\sigma\colon L \to \overline{K}$ über K ein Automorphismus von L ist.

Beispiel 20.7.

1. $\mathbb{C}/\mathbb{R}$ ist normal.
2. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal.

Lemma 20.8. *Eine Körpererweiterug L/K ist normal $\iff$ jedes irreduzible Polynom $f(x) \in K[x]$, das eine Nullstelle in L hat, lässt sich über L als Produkt von Linearfaktoren schreiben.*

Beweis.

$\Leftarrow$) Sei $\sigma\colon L \to \overline{K}$ ein Homomorphismus über K und $\alpha \in L$ ein Element dessen Minimalpolynom wir mit $p(x)$ bezeichnen (insbesondere gilt $p(\alpha) = 0$). Da σ ein Homomorphismus über K ist, wird $\alpha^\sigma \in \overline{L}$ auch eine Nullstelle von $p(x) = p^\sigma(x)$ sein. Da sich $p(x)$ in L als Produkt von Linearfaktoren schreiben lässt, sind alle Nullstellen von $p(x)$ in $\overline{K}$ bereits in L enthalten. Also gilt $\alpha^\sigma \in L$, und somit auch $\sigma(L) \subset L$.

$\Rightarrow$) Sei $f(x) \in K[x]$ ein irreduzibles Polynom und $\alpha \in L$ seine Nullstelle. Sei $\beta \in \overline{K}$ eine weitere Nullstelle von $f(x)$ in $\overline{K}$. Wir möchten zeigen, dass diese bereits in L enthalten ist. In der Tat nach gibt es (nach Lemma 19.3 und Theorem 19.7) einen Homomorphismus $\sigma\colon L \to \overline{K}$ mit der Eigenschaft $\alpha^\sigma = \beta$. Da L/K normal vorausgesetzt ist, folgt daraus $\beta \in L$.

□

Lemma 20.9. *Eine Körpererweiterug L/K ist normal $\iff$ L ist ein Zerfällungskörper einer Familie von Polynomen $\{f_i(x)\}_{i\in I}$.*

Beweis. Übung. □

Teil 7. Intermezzo: Endliche Körper

Sei p eine Primzahl und K ein Körper der Charakteristik p. Erinnerung: Es gibt eine eindeutige Einbettung $\mathbb{F}_p \to K$.

Lemma 20.10. *Die Abbildung*

$$\begin{aligned}\Phi\colon K &\to K\\ x &\mapsto x^p\end{aligned}$$

ist ein Homomorpshismus von Körpern über $\mathbb{F}_p$.

Beweis. Wir zeigen nur, dass gilt $\Phi(x+y) = \Phi(x) + \Phi(y)$. Der Rest ist mehr oder weniger klar und wird als eine kleine Übung gelassen.

Es gilt

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p, \qquad (*)$$

wobei $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Diese Formel bekommt man durch Ausmultiplizieren und ein bisschen Kombinatorik (siehe hier).

Da für jedes $1 \leq k \leq p-1$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!}$$

durch p teilbar ist, sehen wir, dass alle mittlere Terme in $(*)$ verschwinden. Somit gilt

$$(x+y)^p = x^p + y^p,$$

und wir haben $\Phi(x+y) = \Phi(x) + \Phi(y)$.

Die Tatsache, dass Φ ein Homomorphismus über $\mathbb{F}_p \subset K$ ist, d.h. $\alpha^p = \alpha$ für jedes $\alpha \in \mathbb{F}_p$, folgt aus dem Beweis des nächsten Lemmas. □

Lemma 20.11. *Sei L ein Körper mit q Elementen. Dann $\forall \alpha \in L$ gilt $\alpha^q - \alpha = 0$.*

Beweis. Die multiplikative Gruppe L^* hat $q-1$ Elemente. Nach Satz von Lagrange folgt daraus sofort, dass gilt $\alpha^{q-1} = 1$. Durch Multiplizieren mit α bekommen wir $\alpha^q - \alpha = 0$. □

21 27.06.18 — Körper VI

Teil 7. fortgesetzt

Korollar 21.1. *Sei L ein Körper mit q Elementen. Dann ist L der Zerfällungskörper vom Polynom $f(x) = x^q - x \in \mathbb{F}_p[x]$.*

Beweis. Klar. □

Lemma 21.2. *Seien $q = p^n$ und L der Zerfällungskörper vom Polynom $f(x) = x^q - x$ über $\mathbb{F}_p$. Der Körper L kann mit der Menge von Nullstellen vom Polynom $f(x) = x^q - x \in \mathbb{F}_p[x]$ identifiziert werden und hat q Elemente.*

Beweis. Da $a^q = a^{p^n} = \Phi^n(a)$, ist die Menge $L_0 = \{\alpha \in L \mid f(\alpha) = 0\}$ abgeschlossen bezüglich Multiplikation, Addition, etc. Mit anderen Worten ist $L_0 \subset L$ ein Unterkörper.

Es ist klar, dass $\mathbb{F}_p \subset L_0$ und dass L_0 durch Nullstellen von $f(x)$ über $\mathbb{F}_p$ erzeugt wird. Somit ist L_0 der Zerfällungskörper von $f(x) = x^q - x$ über $\mathbb{F}_p$. Daraus folgt, dass gilt $L_0 = L$.

Jetzt müssen wir noch zeigen, dass $f(x) = x^q - x$ genau q unterschiedliche Nullstellen hat. Dafür bemerken wir, dass gilt $f'(x) = qx^{q-1} - 1 = -1$, und somit haben wir $gcd(f(x), f'(x)) = 1$. Nach dem folgenden Lemma sind Nullstellen von $f(x)$ unterschiedlich. □

Lemma 21.3. *Ein Polynom $f(x) \in K[x]$ hat eine mehrfache Nullstelle in $\overline{K}$ $\iff$ $gcd(f(x), f'(x)) \neq 1$.*

Beweis. Sei $a \in \overline{K}$ eine Nullstelle von $f(x)$. Dann gilt $f(x) = (x - a)g(x)$ mit $g(x) \in \overline{K}[x]$. Nach Leibnitz Regel bekommen wir

$$f'(x) = g(x) + (x - a)g'(x),$$

wobei $f'(x)$ die formelle Ableitung von $f(x)$ ist.[10] Daraus folgt

$$(x - a)|f'(x) \iff (x - a)|g(x) \iff (x - a)^2|f(x).$$

□

Korollar 21.4. *Für jedes $q = p^n$ existiert ein eindeutiger (bis auf Isomorphie) Körper mit q Elementen $\mathbb{F}_q$. Dieser ist der Zerfällungskörper von $f(x) = x^q - x$ über $\mathbb{F}_p$.*

Lemma 21.5. *Jeder Endomorphismus von $\mathbb{F}_q$ ist ein Automorphismus.*

Beweis. Die Injektivität gilt für beliebige Körper. Die Surjektivität folgt aus der Injektivität, da die Menge $\mathbb{F}_q$ endlich viele Elemente hat. □

[10] Sei $f(x) = \sum_i a_i x^i$ ein Polynom über einem Körper K. Dann wird die formelle Ableitung $f'(x)$ durch die Formel $f'(x) = \sum_i a_i i x^{i-1}$ definiert.

Korollar 21.6. *Der Homomorphismus $\Phi\colon \mathbb{F}_q \to \mathbb{F}_q$ ist ein Automorphismus. Dieser Automorphismus wird* Frobeniusautomorphismus *gennant.*

Theorem 21.7. *Für $q = p^n$ ist $Aut(\mathbb{F}_q/\mathbb{F}_p)$ eine zyklische Gruppe von Ordnung n, die von Φ erzeugt wird.*

Beweis. Erst zeigen wir, dass die Ordnung von Φ in $Aut(\mathbb{F}_q)$ gleich n ist. Wir haben

$$\Phi^n(a) = a^q = a.$$

Also gilt $\Phi^n = \mathrm{id}$. Andererseits, wenn gilt $\Phi^k = \mathrm{id}$, dann für jedes $a \in \mathbb{F}_q$ haben wir $a^{p^k} = a$, und somit gilt $a \in \mathbb{F}_{p^k}$. Daraus folgt $k \geq n$.

Jetzt zeigen wir, dass beliebiger Automorphismus von $\mathbb{F}_q$ der Form Φ^k ist. Sei $\alpha \in \mathbb{F}_q^*$ ein Erzeuger. Es ist klar, dass gilt $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Daraus folgt $\deg p(x) = n$, wobei $p(x)$ das Minimalpolynom von α ist. Nach Korollar 19.4 bekommen wir $|Aut(\mathbb{F}_q)| \leq n$. □

Teil 8. Separabilitätsgrad

Lemma 21.8. *Sei K/F eine algebraische Körpererweiterung und $\sigma\colon F \to L$ ein Homomorpshismus mit L algebraisch abgeschlossen. Dann ist die Anzahl von Fortsetzungen $\tau\colon K \to L$ von σ auf K unabhängig von σ.*

Beweis. Sei $\sigma'\colon F \to L'$ ein anderer Homomorphismus. Wir betrachten F als Unterkörper F bzw. F' in L bzw. L' (eingebettet durch σ bzw. σ'). Seien $\overline{F}$ bzw. $\overline{F'}$ die algebraische Abschlüsse von F bzw. F' in L bzw. L', und sei $\rho\colon \overline{F} \to \overline{F'}$ ein Isomorphismus (Korollar 19.8). Dann ist $\tau \mapsto \rho \circ \tau$ die gesuchte Bijektion. □

Definition 21.9. Sei K'/K eine endliche Körpererweiterung und $\sigma\colon K' \to L$ ein Homomorphismus mit L algebraisch abgeschlossen. Der Separabilitätsgrad $[K' : K]_s$ von K'/K wird als Anzahl von Fortsetzungen $\tau\colon K' \to L$ von σ auf K' definiert.

22 28.06.18 — Körper VII

Teil 8. fortgesetzt

Lemma 22.1. *Seien $K \subset K' \subset K''$ endliche Körpererweiterungen. Dann gilt*

$$[K'' : K]_s = [K'' : K']_s [K' : K]_s.$$

Beweis. Seien L ein algebraisch abgeschlossener Körper und $\rho\colon K \to L$ ein Homomorphismus. Seien $\sigma_1, \dots, \sigma_n$ mit $n = [K' : K]_s$ alle möglichen Fortsetzungen von ρ auf K', und seien $\tau_{i1}, \dots, \tau_{im}$ mit $m = [K'' : K']_s$ alle mögliche Fortsetzungen von σ_i auf K''.

Erst bemerken wir, dass die Homomorphismen τ_{ij} alle unterschiedlich sind. Wir haben

$$\tau_{ij} = \tau_{kl} \;\Rightarrow\; \sigma_i = \tau_{ij|K'} = \tau_{kl|K'} = \sigma_k \;\Rightarrow\; i = k \;\Rightarrow\; j = l.$$

Sei jetzt $\tau\colon K'' \to L$ eine Fortsetzung von ρ auf K''. Dann gilt $\tau_{|K'} = \sigma_i$ für ein $i \in [1, n]$, und somit gilt $\tau = \tau_{ij}$. □

Lemma 22.2. *Für jede endliche Körpererweiterung K'/K gilt*

$$[K' : K]_s \leq [K' : K].$$

Beweis. Es genügt den Fall $K' = K(\alpha)$ zu betrachten (Übung). Sei also $K' = K(\alpha)$. Dann gilt $[K' : K] = \deg p(x)$ (nach Lemma 17.5) und $[K' : K]_s \leq \deg p(x)$ (nach Korollar 19.4). □

Korollar 22.3. *Seien $K \subset K' \subset K''$ endliche Körpererweiterungen. Dann gilt*

$$[K'' : K]_s = [K'' : K] \iff [K' : K]_s = [K' : K] \text{ und } [K'' : K']_s = [K'' : K'].$$

Teil 9. Separable Körpererweiterungen

Definition 22.4. Ein irreduzibles Polynom $f(x) \in K[x]$ heißt separabel, wenn $f(x)$ keine mehrfachen Nullstellen in $\overline{K}$ hat.

Lemma 22.5. *Ein irreduzibles Polynom $f(x) \in K[x]$ ist nicht separabel* $\iff$ $\operatorname{char}(K) = p$ *und $f(x) = g(x^{p^n})$ für ein irreduzibles separables Polynom $g(x) \in K[x]$.*[11]

Beweis. $\Rightarrow$) Nach Lemma 21.3 hat $f(x)$ eine mehrfache Nullstelle in $\overline{K}$ genau dann, wenn gilt $gcd(f(x), f'(x)) \neq 1$. Da $f(x)$ irreduzibel ist, folgt daraus $gcd(f(x), f'(x)) = f(x)$.[12]

Es ist offensichtlich, dass gilt $\deg f'(x) < \deg f(x)$. Somit folgt aus $gcd(f(x), f'(x)) = f(x)$, dass wir haben $f'(x) = 0$. Daraus folgt: $\operatorname{char}(K) = p > 0$ und $f(x) = f_1(x^p)$ mit $f_1(x) \in K[x]$. Da $f(x)$ irreduzibel ist, ist auch $f_1(x)$ irreduzibel.

[11] Mit $g(x^{p^n})$ wird hier und im Folgenden $g(x^{(p^n)})$ gemeint.

[12] Hier haben wir Folgendes benutzt: Seien $f(x), g(x) \in K[x]$ zwei Polynome, und sei $h(x) = gcd_{\overline{K}[x]}(f(x), g(x))$ der GGT von $f(x)$ und $g(x)$ in $\overline{K}[x]$. Dann gilt bereits: $h(x) \in K[x]$.

Solange $f_1(x)$ nicht separabel ist, kann man das obige Vorgehen wiederholen. Da durch jedes Iterieren der Grad vom Poylnom $f_1(x)$ sinkt, wird dieses Vorgehen in endlich vielen Interationen aufhören. Als Resultat bekommen wir $f(x) = g(x^{p^n})$ mit $g(x)$ irreduzibel und separabel.

$\Leftarrow$) Übung. □

Definition 22.6. Sei L/K eine Körpererweiterung. Ein algebraisches Element $\alpha \in L$ heißt separabel, wenn sein Minimalpolynom separabel ist. Eine algebraische Körpererweiterung L/K heißt separabel, wenn jedes Element $\alpha \in L$ separabel ist.

Korollar 22.7. *Wenn gilt* $\mathrm{char}(K) = 0$*, dann ist jede algebraische Körpererweiterung* L/K *separabel.*

Lemma 22.8. *Sei* K *ein Körper mit* $\mathrm{char}(K) = p > 0$*. Ein Element* α *ist separabel über* K $\iff$ *es existiert ein Polynom* $f(x) \in K[x]$ *ohne mehrfachen Nullstellen in* $\overline{K}$*, sodass gilt* $f(\alpha) = 0$*.*

Beweis. $\Rightarrow$) Wir können das Minimalpolynom von α als $f(x)$ nehmen.

$\Leftarrow$) Sei $p(x) \in K[x]$ das Minimalpolynom von α. Da $p(x)|f(x)$ und $f(x)$ keine mehrfachen Nullstellen in $\overline{K}$ hat, folgt es, dass auch $p(x)$ keine mehrfachen Nullstellen in $\overline{K}$ hat. □

Lemma 22.9. *Seien* $K \subset K' \subset K''$ *Körpererweiterungen. Dann gilt:*

$$K''/K \text{ ist separabel } \implies K''/K' \text{ und } K'/K \text{ sind separabel.}$$

Beweis. Es folgt sofort aus der Separabilität von K''/K , dass K'/K separabel ist. Um die Separabilität von K''/K' zu beweisen, wendet man das obige Lemma an. □

Lemma 22.10. *Sei* K *ein Körper mit* $\mathrm{char}(K) = p > 0$*, und seien* L/K *eine Körpererweiterung und* $\alpha \in L$ *ein algebraisches Element mit dem Minimalpolynom* $f(x) \in K[x]$*. Weiter sei* $g(x) \in K[x]$ *ein inrreduzibles und separables Polynom mit der Eigenschaft* $f(x) = g(x^{p^m})$ *(vgl. Lemma 22.5). Dann ist* α^{p^m} *separabel über* K *und* $[K(\alpha) : K]_s = \deg g(x)$*. Insbesondere gilt es* $[K(\alpha) : K] = p^m[K(\alpha) : K]_s$*.*

Beweis. Seien $\beta_1, \ldots, \beta_n$ die Nullstellen von $g(x)$ in $\overline{K} \supset L \supset K$. Für jedes β_i existiert ein eindeutiges $\alpha_i \in \overline{K}$ mit der Eigenschaft $\alpha_i^{p^m} = \beta_i$.[13] Wir haben

$$f(x) = g(x^{p^m}) = \prod_{i=1}^{n}(x^{p^m} - \alpha_i^{p^m}) = \prod_{i=1}^{n}(x - \alpha_i)^{p^m}.$$

Daraus folgt $[K(\alpha) : K]_s = n = \deg g(x)$. Weiter gilt $[K(\alpha) : K] = \deg f(x) = p^m \deg g(x) = p^m[K(\alpha) : K]_s$.

Das Element α^{p^m} ist separabel, weil es eine Nullstelle eines separables Polynoms $g(x)$ ist. □

[13] $\alpha_i^{p^m} = \alpha'^{p^m}_i \;\Rightarrow\; \alpha_i^{p^m} - \alpha'^{p^m}_i = 0 \;\Rightarrow\; (\alpha_i - \alpha'_i)^{p^m} = 0 \;\Rightarrow\; \alpha_i = \alpha'_i$.

Korollar 22.11. *α ist separabel* $\iff [K(\alpha) : K] = [K(\alpha) : K]_s$.

Beweis. Übung. □

23 04.07.18 — Körper VIII

Teil 9. fortgesetzt

Theorem 23.1. *Eine endliche Körpererweterung K'/K ist separabel* $\iff$

$$[K' : K] = [K' : K]_s.$$

Beweis. $\Rightarrow$) Sei K'/K eine endliche separable Körpererweiterung. Für ein Element $\alpha \in K' \setminus K$ betrachten wir Körpererweiterungen $K \subset K(\alpha) \subset K'$. Nach Lemma 22.9 sind $K \subset K(\alpha)$ und $K(\alpha) \subset K'$ separabel. Dann gilt nach Korollar 22.11 $[K(\alpha) : K] = [K(\alpha) : K]_s$. Die Aussage folgt jetzt nach Induktion und Multiplikativität von Grad und Separabilitätsgrad.

$\Leftarrow$) Sei $[K' : K] = [K' : K]_s$. Dann gilt für jedes $\alpha \in K' \setminus K$ nach Korollar 22.3 $[K(\alpha) : K] = [K(\alpha) : K]_s$. Somit ist α separabel nach Korllar 22.11. □

Korollar 23.2. *$K(\alpha_1, \dots, \alpha_n)/K$ ist separabel* $\iff$ *$\alpha_1, \dots, \alpha_n$ sind separabel über K.*

Beweis. $\Rightarrow$) Klar.

$\Leftarrow$) Betrachten wir $K(\alpha_1, \dots, \alpha_n)/K$ als eine konsekutive Körpererweiterung

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \dots, \alpha_n).$$

Für jede zwei konsekutive Körper ist die Erweiterung separabel, und somit ist der Grad dem Separabilitätsgrad gleich (Korollar 22.11). Daraus folgt

$$[K(\alpha_1, \dots, \alpha_n) : K] = [K(\alpha_1, \dots, \alpha_n) : K]_s.$$

Jetzt nach Theorem 23.1 bekommen wir die Separabilität von $K(\alpha_1, \dots, \alpha_n)/K$. □

Korollar 23.3. *Seien $K \subset K' \subset K''$ Körpererweiterungen. Dann gilt:*

$$K''/K \text{ ist separabel} \iff K''/K' \text{ und } K'/K \text{ sind separabel.}$$

Beweis. $\Rightarrow$) Schon bekannt.

$\Leftarrow$) Seien $K \subset K' \subset K''$ die Körpererweiterungen, $\alpha \in K''$ ein Element, und $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \subset K'[x]$ das Minimalpolynom von α über K'.

Da die Elemente $a_0, \dots, a_{n-1}$ separabel über K sind (nach Voraussetzung), ist die Körpererweiterung $K \subset K(a_0, \dots, a_{n-1})$ separabel nach Korollar 23.2. Weiter ist α separabel über $K(a_0, \dots, a_{n-1}) \subset K'$ (Lemma 22.8). Daraus folgt

$$[K(a_0, \dots, a_{n-1}, \alpha) : K] = [K(a_0, \dots, a_{n-1}, \alpha) : K]_s,$$

und somit ist α separabel über K. □

Teil 10. Rein-inseparable Körpererweiterungen

Lemma 23.4. *Sei L/K eine endliche Körpererweiterung. Dann wird $[L:K]$ durch $[L:K]_s$ geteilt.*

Beweis. In Charakteristik 0 ist klar. In positiver Charakteristik folgt aus Lemma 22.10. □

Definition 23.5. Sei L/K eine endliche Körpererweiterung. Die ganze Zahl

$$[L:K]_i := [L:K]/[L:K]_s$$

nennt man Inseparabilitätsgrad von L/K.

Lemma 23.6. *Sei L/K eine endliche Körpererweiterung. Wenn $\mathrm{char}(K) = 0$, dann gilt $[L:K]_i = 1$. Wenn $\mathrm{char}(K) = p$, dann gilt $[L:K]_i = p^m$ für ein $m \in \mathbb{Z}_{\geq 0}$.*[14]

Beweis. In Charakteristik 0 ist klar. In positiver Charakteristik folgt aus Lemma 22.10. □

Definition 23.7. Ein Element $\alpha \in L$ heißt rein-inseparabel über K, wenn gilt $\alpha^{p^m} \in K$ für ein $m \in \mathbb{Z}_{\geq 0}$. Die Körpererweiterung L/K heißt rein-inseparabel, wenn jedes Element in L rein-inseparabel über K ist.[15]

Lemma 23.8. *Ein Element $\alpha \in L$ ist rein-inseparabel über K $\iff$ das Minimalpolynom von α über K ist der Form $x^{p^m} - a$ mit $a \in K$ und $m \in \mathbb{Z}_{\geq 0}$.*[16]

Beweis. $\Leftarrow$) Folgt sofort aus der Definition.

$\Rightarrow$) Sei $g(x) \in K[x]$ das Minimalpolynom von α, und sei $m > 0$ die kleinste positive Zahl, so dass gilt $\alpha^{p^m} \in K$. Dann liegt $f(x) = (x-\alpha)^{p^m} = x^{p^m} - \alpha^{p^m}$ in $K[x]$. Daraus folgt, dass das Minimalpolynom $g(x)$ das Polynom $f(x)$ teilt, d.h. wir haben $g(x) = (x-\alpha)^n$ mit $n \leq p^m$. Wir haben

$$g(x) = (x-\alpha)^n = \left((x-\alpha)^{p^{m'}}\right)^r = \left(x^{p^{m'}} - \alpha^{p^{m'}}\right)^r = x^n - r\alpha^{p^{m'}} x^{(r-1)p^{m'}} + \ldots,$$

wobei $n = rp^{m'}$ und $gcd(p, m') = 1$. Da $g(x)$ Koeffizienten in K hat, bekommen wir $\alpha^{p^{m'}} \in K$. Da m minimal gewählt wurde, haben wir $m = m'$, $r = 1$ und $g(x) = f(x)$. □

Korollar 23.9. *L/K ist rein-inseparabel $\iff$ $\forall \alpha \in L$ ist das Minimalpolynom von α der Form $x^{p^m} - a$ für ein $a \in K$ und ein $m \in \mathbb{Z}_{\geq 0}$.*[17]

Lemma 23.10. *Eine endliche Körpererweiterung L/K ist rein-inseparabel $\iff$ $[L:K]_s = 1$.*

[14] In der Vorlesung stand hier wahrscheinlich $\mathbb{Z}_{>0}$. Natürlich brauchen wir $\mathbb{Z}_{\geq 0}$ um den Fall $m = 0$ (separable Körpererweiterungen) einzuschließen.

[15] In der Vorlesung stand hier wahrscheinlich $\mathbb{Z}_{>0}$. Nochmals sollte hier $\mathbb{Z}_{\geq 0}$ stehen. Insbesondere ist jedes Element aus K rein-inseparabel über K, und somit ist die triviale Körpererweiterung $L = K$ rein-inseparabel!

[16] In der Vorlesung stand hier wahrscheinlich $\mathbb{Z}_{>0}$. Nochmals sollte hier $\mathbb{Z}_{\geq 0}$ stehen.

[17] In der Vorlesung stand hier wahrscheinlich $\mathbb{Z}_{>0}$. Nochmals sollte hier $\mathbb{Z}_{\geq 0}$ stehen.

Beweis. $\Rightarrow$) Sei L/K endlich und rein-inseparabel. Es genügt, den Fall $L = K(\alpha)$ zu betrachten (Übung). Nach Lemma 23.8 ist das Minimalpolynom von α der Form $x^{p^m} - a$. Aus Lemma 22.10 folgern wir $[K(\alpha) : K]_s = 1$.

$\Leftarrow$) Wenn gilt $[L : K]_s = 1$, dann gilt $[K(\alpha) : K]_s = 1$ für jedes $\alpha \in L$. Nach Lemma 22.10 ist das Minimalpolynom von α der Form $x^{p^m} - a$, und somit ist α rein-inseparabel nach Lemma 23.8. □

Korollar 23.11. *Seien $K \subset K' \subset K''$ Körpererweiterungen. Dann gilt:*

$$K''/K \text{ ist rein-inseparabel} \iff K''/K' \text{ und } K'/K \text{ sind rein-inseparabel.}$$

24 05.07.18 — Galoistheorie I

Teil 11. Separabler Abschluss

Lemma 24.1. *Sei L/K eine Körpererweiterung. Die Teilmenge*

$$L^{sep} := \{\alpha \in L \mid \alpha \text{ ist separabel über } K\}$$

ist ein Unterkörper von L, und die Körpererweiterung $K \subset L^{sep}$ ist separabel.

Beweis. Seien $\alpha, \beta \in L^{sep}$. Dann ist $K(\alpha, \beta)/K$ eine separable Körpererweiterung (Korollar 23.2) und ist somit in L^{sep} enthalten. Daraus folgt, dass $\alpha + \beta, \alpha\beta, \dots$ auch in L^{sep} liegen. Somit ist L^{sep} ein Unterkörper von L. Die Separabilität gilt nach Definition. □

Definition 24.2. Der Körper L^{sep} wird separabler Abschluss von K in L genannt.

Lemma 24.3. *Die Körpererweiterung L^{sep}/K ist separabel und L/L^{sep} rein-inseparabel.*

Beweis. Die erste Aussage ist klar. Wir zeigen die zweite. Sei $\alpha \in L$ ein Element. Dann gibt es ein m, so dass α^{p^m} separabel über K ist (Lemma 22.10) und somit in L^{sep} liegt. Somit ist α rein-inseparabel über L^{sep}. □

Bemerkung 24.4. Somit kann man jede Körpererweiterung L/K als Komposition einer separablen und einer rein-inseparablen darstellen

$$K \subset L^{sep} \subset L.$$

Theorem 24.5. *Seien L/K eine normale Körpererweiterung und $G = Aut(L/K)$. Dann ist die Teilmenge*

$$L^G := \{x \in L \mid Gx = x\}$$

ein Unterkörper von L. Die Körpererweiterung L/L^G ist separabel und L^G/K rein-inseparablel.

Beweis. 1. Sei $\alpha \in L$. Da die Bahn von α endlich ist (Übungsblatt), gibt es Elemente $\{\sigma_0 = e, \dots, \sigma_{n-1}\} \subset G$, so dass

$$Orb(\alpha) = \{\sigma_0\alpha = \alpha, \dots, \sigma_{n-1}\alpha\}.$$

Betrachten wir nun das Polynom

$$p(x) = \prod_{i=0}^{n-1}(x - \alpha^{\sigma_i}).$$

Es ist leicht zu sehen, dass für jedes $\sigma \in G$ gilt $p^\sigma(x) = p(x)$, und somit gilt auch $p(x) \in L^G[x]$. Nach Definition hat $p(x)$ keine mehrfachen Nullstellen und $p(\alpha) = 0$. Daraus folgt, dass α separabel über L^G ist (Lemma 22.8), und somit ist L/L^G eine separable Körpererweiterung.

2. Betrachten wir jetzt ein Element $\alpha \in L^G$, und sei $\sigma\colon K(\alpha) \to \overline{K}$ ein Homomorphismus und $\tau\colon L \to \overline{K}$ eine Fortsetzung von σ (Theorem 19.7). Dann gilt $\tau \in G = Aut(L/K)$, da L/K normal ist. Da $\alpha \in L^G$ folgt daraus, dass gilt $\alpha^\tau = \alpha^\sigma = \alpha$. Dann gilt $\sigma = Id_{K(\alpha)}$, und somit bekommen wir $[K(\alpha) : K]_s = 1$ und α ist rein-inseparabel über K (Lemma 23.10). □

Definition 24.6. Ein Körper heißt perfekt, wenn entweder $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) = p$ und $\Phi(K) = K$, wobei Φ der Frobenius ist.

Korollar 24.7. *Algebraische Erweiterungen von perfekten Körpern sind separabel.* [18]

Beweis. Sei L/K eine algebraische Erweiterung von K mit K perfekt, und sei $\alpha \in L$ ein Element. Nach Lemma 23.8 ist α rein-inseparabel genau dann, wenn das Minimalpolynom von α der Form $x^{p^m} - a$ mit $a \in K$ und $m \geq 0$ ist. Da K perfekt ist, gibt es ein $\alpha \in K$, so dass $\alpha^{p^m} = a$. Somit hat das Minimalpolynom von α eine Nullstelle in K, was seiner Irreduzibilität widerspricht. Also kann α nicht rein-inseparabel sein. Somit hat K keine rein-inseparablen Erweiterungen.

Sei nun L/K eine beliebige algebraische Erweiterung. Es existiert eine Erweiterung $L' \supset L \supset K$, sodass L'/K normal ist. Dann ist L'/K separabel (Theorem 24.6), und somit ist auch L/K separabel. □

Teil 1. Hauptsatz der Galoistheorie

Definition 24.8.

1. Eine Körpererweiterung L/K heißt Galoiserweiterung, wenn L/K normal und separabel ist.
2. Die Automorphismengruppe $\mathrm{Aut}(L/K)$ heißt dann Galoisgruppe von L über K und wird mit $\mathrm{Gal}(L/K)$ bezeichnet.
3. Jeder Untergruppe $H \subset \mathrm{Gal}(L/K)$ ordnet man ein Unterkörper
$$L^H := \{\alpha \in L \mid \forall \sigma \in H \text{ gilt } \alpha^\sigma = \alpha\} \subset L$$
zu.
4. Jedem Zwischenkörper $K \subset F \subset L$ ordnet man eine Untergruppe $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ zu.

Der Hauptsatz der Galoistheorie ist Folgendes:

Theorem 24.9. *Sei L/K eine endliche Galoiserewiterung. Dann liefern die Zuordnungen*
$$\begin{aligned} H &\mapsto L^H \\ \mathrm{Gal}(L/F) &\leftarrow\!\shortmid F \end{aligned}$$
zueinander inverse inklusionsumkehrende Bijektionen
$$\{\textit{Zwischekörper von } L/K\} \leftrightarrow \{\textit{Untergruppen von } \mathrm{Gal}(L/K)\}.$$

[18] Dieser Korollar und die obige Definition wurden in der Vorlesung weggelassen.

Beweis. Injektivität: Korollar 24.12. Surjektivität: Korollar 25.7.

□

Lemma 24.10. *Sei L/K eine Galoiserweiterung und $G = \mathrm{Gal}(L/K)$. Dann gilt $L^G = K$.*

Beweis. Da L/K normal ist, können wir Theorem 24.5 anwenden und bekommen, dass L/L^G separabel ist, und L^G/K rein-inseparabel ist. Da L/K eine Galoiserweiterung ist, ist L/K separabel. Daraus folgern wir sofort $L^G = K$. □

Lemma 24.11. *Wenn L/K eine Galoiserweiterung ist und $K \subset F \subset L$. Dann ist L/F auch Galoiserweiterung.*

Beweis. Da L/K normal und separabel ist, ist auch L/F normal und separabel (Korollar 23.3). □

Korollar 24.12. *Wenn L/K eine Galoiserweiterung ist, ist die Abbildung $F \mapsto \mathrm{Gal}(L/F)$ injektiv.*

Beweis. Sei F ein Zwischenkörper $K \subset F \subset L$. Da L/F eine Galoiserweiterung ist (Lemma 24.11), gilt $L^{\mathrm{Gal}(L/F)} = F$ (Lemma 24.10). D.h. wir können den Körper F aus $\mathrm{Gal}(L/F)$ rekonstruieren. □

Korollar 24.13. *Für die Injektivität von $F \mapsto \mathrm{Gal}(L/F)$ haben wir nicht benutzt, dass L/K endlich ist. Diese gilt somit für beliebige Galoiserweiterungen.*

25 11.07.18 — Galoistheorie II

Teil 2. Satz vom primitiven Element

Definition 25.1. Sei L/K eine algebraische Körpererweiterung. Ein Element $\alpha \in L$ heißt primitiv, wenn gilt $L = K(\alpha)$.

Beispiel 25.2.

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ hat ein primitives Element (sofort klar nach Definition).
2. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ hat auch ein primitives Element (folgt aus Lemma 25.5, vgl. Übungsblatt).
3. Unendliche Körpererweiterungen haben kein primitives Element.

Lemma 25.3. *Wenn für eine Körpererweiterung L/K ein primitives Element $\alpha \in L$ existiert, dann ist L/K eine endliche Körpererweiterung und die Anzahl von Zwischenkörper $K \subset F \subset L$ ist auch endlich.*

Beweis. Nach Voraussetzung haben wir $L = K(\alpha)$.

Sei $p(x) \in K[x]$ das Minimalpolynom von α über K. Die erste Aussage folgt sofort aus

$$[K(\alpha) : K] = \deg p(x).$$

Somit bleibt uns nur die zweite Aussage zu beweisen.

Sei F ein Zwischenkörper, d.h. wir haben $K \subset F \subset L$, und sei $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ das Minimalpolynom von α über F. Wir werden gleich sehen, dass gilt

$$F = K(a_0, \ldots, a_{n-1}),$$

und somit ist ein Zwischenkörper F von $K(\alpha)/K$ durch das Minimalpolynom von α über F eindeutig bestimmt.

Erstens haben wir die Inklusion $K(a_0, \ldots, a_{n-1}) \subset F$, da gilt $a_i \in F$. Bemerken wir, dass das Polynom $q(x)$ ist auch das Minimalpolynom von α über $K(a_0, \ldots, a_{n-1})$ (Übung). Daraus folgt

$$[K(\alpha) : K(a_0, \ldots, a_{n-1})] = n = [K(\alpha) : F],$$

und somit gilt $K(a_0, \ldots, a_{n-1}) \subset F$.

Jetzt möchten wir zeigen, dass es nur endlich viele Möglichkeiten für das Minimalpolynom $q(x)$ eines Zwischenkörpers gibt. Dafür bemerken wir, dass gilt $p(\alpha) = 0$ und $p(x) \in K[x] \subset F[x]$. Daraus folgt, dass $q(x)$ in $F[x]$ das Polynom $p(x)$ teilt. Somit gilt auch $q(x)|p(x)$ in $L[x] \supset F[x]$.

Jetzt um zur Aussage zu beweisen, reicht es zu zeigen, dass $p(x)$ in $L(x)$ endlich viele Teiler hat. Weiter genügt es zu zeigen, dass $p(x)$ in $\overline{L}(x)$ endlich viele Teiler hat. Es ist klar, dass die Anzahl von Teiler von $p(x)$ in $\overline{L}(x)$ durch 2^m begrenzt ist, wobei $m = \deg p(x)$. □

Die Umkehrung gilt auch!

Lemma 25.4. *Sei L/K eine endliche Körpererweiterung mit der Eigenschaft, dass die Anzahl von Zwischenkörper $K \subset F \subset L$ endlich ist. Dann hat L/K ein primitives Element.*

Beweis. Wenn K ein endlicher Körper ist, ist L auch endlich. Es ist klar, dass die Anzahl von Zwischenkörper automatisch endlich ist. Als ein primitives Element kann man in diesem Fall einen Erzeuger der Einheitsgruppe L^* nehmen, die bekanntermaßen zyklisch ist.

Sei jetzt K unendlich. Es genügt den Fall $L = K(\alpha, \beta)$ zu betrachten (Übung: Induktion nach Anzahl von Erzeuger von L/K). D.d. wir müssen zeigen, dass für $L = K(\alpha, \beta)$ ein $\gamma \in L$ existiert, sodass gilt $L = K(\gamma)$. Wir werden nach γ der Form $\gamma = \alpha + c\beta$ mit $c \in K$ suchen.

Es ist klar, dass $K(\alpha + c\beta)$ ein Zwischenkörper von L/K ist. Da K unendlich ist, und es nach Voraussetzung nur endlich viele Zwischenkörper gibt, existieren $c_1 \neq c_2 \in K$ mit der Eigenschaft $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Dann haben wir haben

$$\begin{aligned}\beta &= \Big((\alpha + c_1\beta) - (\alpha + c_2\beta)\Big)/(c_1 - c_2),\\ \alpha &= (\alpha + c_1\beta) - c_1\beta,\end{aligned}$$

und somit liegen α und β in $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Daraus folgt

$$K(\alpha + c_1\beta) = K(\alpha + c_2\beta) = K(\alpha, \beta).$$

□

Lemma 25.5 (Satz vom primitiven Element)**.** *Sei L/K eine endliche separable Körpererweiterung. Dann existiert ein primitives Element.*

Beweis. Es genügt den Fall vom unendlichen Körper K und $L = K(\alpha, \beta)$ zu betrachten (wie im Beweis oben).

Sei $n = [L : K] = [L : K]_s$, und seien $\sigma_1, \ldots, \sigma_n$ unterschiedliche K-Homomorphisme $L \to \overline{K}$.

Es existiert ein $c \in K$ (Übung), so dass $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ für $i \neq j$. D.h. für $\gamma = \alpha + c\beta$ sind $\sigma_i(\gamma) \in \overline{K}$ alle unterschiedlich. Somit sind $\{\sigma_1, \ldots, \sigma_n\}$ betrachtet als K-Homomorphisme $K(\gamma) \to \overline{K}$ auch alle unterschiedlich. Daraus folgt

$$[K(\gamma) : K] \geq [K(\gamma) : K]_s \geq n = [L : K],$$

und somit gilt $K(\gamma) = L$. □

Korollar 25.6. *Sei L/K eine separable Körpererweiterung mit $[K(\alpha) : K] \leq n$ für jedes $\alpha \in L$. Dann gilt $[L : K] \leq n$.*

Beweis. Betrachten wir ein $\alpha \in L$, sodass die Zahl $[K(\alpha) : K] = m$ maximal ist. Wir werden zeigen, dass gilt $L = K(\alpha)$.

Sei $\beta \in L$ mit $\beta \notin K(\alpha)$. Dann nach Lemma 25.5 existiert ein γ, sodass $K(\gamma) = K(\alpha, \beta)$. Dann gilt

$$[K(\gamma) : K] = [K(\alpha, \beta) : K] > [K(\alpha) : K],$$

was der Maximalität von $[K(\alpha) : K]$ widerspricht. Draus folgern wir: $L = K(\alpha)$ und $[L : K] = m \leq n$. □

26 12.07.18 — Galoistheorie III

Teil 3. Beweis des Hauptsatzes: fortgesetzt

Lemma 26.1. *Sei L/K eine endliche Körpererweiterung. Dann gilt*

1. $|\operatorname{Aut}(L/K)| \leq [L:K]_s \leq [L:K]$.
2. *L/K ist eine endliche Galoiserweiterung* $\iff |\operatorname{Aut}(L/K)| = [L:K]$.

Beweis. Gemacht in der Vorlesung. □

Lemma 26.2. *Sei L ein Körper und $G \subset \operatorname{Aut}(L)$ eine endliche Automorphismengruppe mit $|G| = n$ und $F = L^G$. Dann ist L/F eine endliche Galoiserweiterung mit $G = \operatorname{Gal}(L/F)$ und $[L:K] = n$.*

Beweis. Seien $\alpha \in L$ und $Orb(\alpha) = \{\alpha_1, \ldots, \alpha_m\}$. Es ist klar, dass für das Polynom

$$f(x) = \prod_{i=1}^{m} (x - \alpha_i)$$

gilt $f^\sigma(x) = f(x)$ für jedes $\sigma \in G$, d.h. $f(x) \in F[x]$. Andererseits haben wir $f(\alpha) = 0$, da gilt $\alpha \in \{\alpha_1, \ldots, \alpha_m\}$.

Daraus folgt, dass $f(x)$ wird durch das Minimalpolynom $p(x)$ von α über F geteilt. Da $f(x)$ lässt sich über L als Produkt von Linearfaktoren schreiben und keine mehrfache Nullestellen hat, gilt dasselbe für $p(x)$.

Da $\alpha \in L$ beliebig war, folgt daraus, dass L/F separabel und normal ist, und somit eine Galoiserweiterung ist.

Weiter folgt aus den obigen Überlegungen, dass für jedes $\alpha \in L$ gilt $[F(\alpha):F] \leq n$. Jetzt folgt nach Korollar 25.6 daraus $[L:F] \leq n$.

Andererseits gilt $n = |G| \leq [L:F]_s \leq [L:F]$ (Lemma 26.1 angewendet an L/F). Somit bekommen wir $n = [L:F]_s = [L:F]$ und $G = \operatorname{Aut}(L/F) = \operatorname{Gal}(L/F)$. □

Korollar 26.3. *Sei L/K eine endliche Galoiserweiterung. Dann ist die Abbildung $F \mapsto \operatorname{Gal}(L/F)$ surjektiv.*

Beweis. Sei $H \subset \operatorname{Gal}(L/K) = \operatorname{Aut}(L/K)$ eine Untergruppe. Nach Lemma 26.2 haben wir $H = \operatorname{Aut}(L/L^H)$. Daraus folgt die Surjektivität. □

Somit ist der Beweis des Hauptsatzes 24.9 abgeschlossen.

Teil 4. Ergänzungen

Notation: L/K eine endliche Galoiserweiterung, $K \subset F \subset L$ ein Zwischenkörper.

Bisher haben wir gezeigt, dass für eine endliche Galoiserweiterung L/K ist die Abbildung

$$\begin{aligned} &\{\text{Zwischekörper von } L/K\} \to \{\text{Untergruppen von } \mathrm{Gal}(L/K)\} \qquad (*) \\ &F \mapsto \mathrm{Gal}(L/F) \end{aligned}$$

eine Bijektion. Bemerken wir jetzt, dass wir auf beiden Seiten noch eine Wirkung von $G = \mathrm{Gal}(L/K)$ haben: 1) Auf ihren Untergruppen wirkt G durch Konjugation: $H \mapsto^{\sigma} H^{\sigma^{-1}}$ 2) Auf Unterkörper: $F \mapsto \sigma(F)$.

Lemma 26.4. *Die Abbildung* $(*)$ *ist eine Abbildung von G-Mengen.*

Beweis. Sei $\sigma \in G = \mathrm{Aut}(L/K)$ und $H \subset G$ eine Untergruppe. Dann gilt

$$\begin{aligned} &L^{\sigma H \sigma^{-1}} = \{\alpha \in L \mid \forall h \in H \quad \sigma h \sigma^{-1}(\alpha) = \alpha\} = \\ &= \{\alpha \in L \mid \forall h \in H \quad h\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)\} = \{\alpha \in L \mid \sigma^{-1}(\alpha) \in L^H\} = \\ &= \{\alpha = \sigma(\beta) \mid \beta \in L^H\} = (L^H)^{\sigma}. \end{aligned}$$

□

Lemma 26.5.

1. *Die Zwischenerweiterung F/K ist normal $\iff$ die Untergruppe $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ ist ein Normalteiler.*
2. *Wenn F/K normal ist, dann gilt $\mathrm{Gal}(F/K) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$*

Beweis. Ohne Beweis. □

Lemma 26.6. *Seien F, F' Zwischenkörper. Dann gilt*

$$F \subset F' \iff \mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F).$$

Beweis. Übung. □