Einführung in die Algebra

Thomas Nikolaus

8. Juli 2021

Inhaltsverzeichnis

1 Einführung

Was ist Algebra? Hier ist die Wikipedia Definition:

> Die Algebra (von arabisch al-gabr „das Zusammenfügen gebrochener Teile“) ist eines der grundlegenden Teilgebiete der Mathematik; es befasst sich mit den Eigenschaften von Rechenoperationen. Im Volksmund wird Algebra häufig als das Rechnen mit Unbekannten in Gleichungen bezeichnet (zum Beispiel $x + 1 = 2$).

Wir interessieren uns in diesem Kurs auch für etwas kompliziertere Gleichungen, zum Beispiel

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0 \qquad a_i \in \mathbb{C} \quad a_n \neq 0 \ .$$

Wir wollen alle Lösungen dieser Gleichung finden/beschreiben.

Frage 1.1. *Gibt es eine Lösungsformel für diese Gleichung?*

Für $n = 1$ lässt sich diese Gleichung offensichtlich einfach lösen. Für $n = 2$ kennen wir ebenfalls die Lösungsformel:

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0 a_2}}{2a_2} \ .$$

Es gibt auch für $n = 3$ und $n = 4$ Lösungsformeln in Termen von Radikalen, d.h. Wurzeln, Addition und Multiplikation, gefunden von del Ferro (1515) und Ferrari (1545). Einer der Hauptsätze dieser Vorlesung wird sein, dass es für $n \geq 5$ keine allgmeiner Lösungsformel in Termen von Radikalen geben kann.

Dies schließt natürlich nicht aus, dass es für spezielle Gleichungen, wie zum Beispiel $x^n - a_0 = 0$ dennoch Lösungsformeln gibt (was sind die Lösungen?). Genauer definiert man für jedes Polynom

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

eine Gruppe $\mathrm{Gal}(p)$, gennant die *Galois Gruppe* des Polynoms wie folgt. Wir erinnern daran, dass ein Körperautomorphismus von $\mathbb{C}$ eine bijektiven Abbildung $\sigma : \mathbb{C} \to \mathbb{C}$ ist die

$$\begin{aligned} \sigma(a+b) &= \sigma(a) + \sigma(b) & \sigma(0) &= 0 \\ \sigma(ab) &= \sigma(a)\sigma(b) & \sigma(1) &= 1 \end{aligned}$$

erfüllt. Wir betrachten die Automorphismen σ mit $\sigma(a_i) = a_i$. Jede Nullstelle x von p wird wegen

$$p(\sigma(x)) = \sigma(p(x)) = \sigma(0) = 0$$

auf eine Nullstelle abgebildet. Seien

$$N_p = \{a_1, ..., a_k\} \subseteq \mathbb{C}$$

die komplexen Nullstellen des Polynoms p, welche nach dem Fundamentalsatz der Algebra existieren. Dann induziert σ eine Permutation dieser Menge und die Galois Gruppe ist die Menge aller so entstehenden Permutationen von N_p. Dies wird eine Gruppe mittels der Komposition.

Satz 1.2 (Galois)**.** *Die Gleichung $p(x) = 0$ is genau dann durch Radikale lösbar, wenn die Galois Gruppe* $\mathrm{Gal}(p)$ *auflösbar im Sinne der Gruppentheorie ist.*

Wir werden den Begriff der Auflösbarkeit von Gruppen einführen genauer untersuchen. Der Satz führt das Studium der Auflösbarkeit auf das Studium von Gruppen zurück. Insbesondere werden wir sehen, dass eine Allgmeine Gleichung n-ten Grades als Galois Gruppe die symmetrische Gruppe Σ_n hat. Wir werden sehen, dass diese für $n \geq 5$ nicht auflösbar ist und daher dass es keine Lösungsformel geben kann.

2 Konstruktionen mit Zirkel und Lineal

Wir starten mit einer Menge $M \subseteq \mathbb{R}^2 \cong \mathbb{C}$ von Punkten in der Ebene. Die Frage ist welche weiteren Punkte in $\mathbb{R}^2$ daraus mittels Zirkel und Lineal konstruiert werden können. Genauer sind dabei folgende Manöver erlaubt:

1. Durch je zwei konstruierte oder vorgegebene Punkte kann man eine Gerade legen.

2. Um jeden konstruierten oder vorgegebenen Punkt kann man einen Kreis schlagen mit einem Radius, den man als Verbindungsstrecke zweier Punkte in M abgreift.

3. Schnittpunkte von Kreisen mit Kreisen, von Kreisen und Geraden und von Geraden mit Geraden sind konstruierte Punkte.

Wir nehmen jetzt an, dass $M = \{0, 1\}$. Dann können wir folgende klassische Fragen stellen:

Frage 2.1 (Quadratur des Kreises)**.** *Kann man ein Quadrat mit gleichen Flächeninhalt wie der Einheitskreis konstruieren?*

Frage 2.2 (Konstruktion des regelmäßigen n-Ecks)**.** *Kann man die Ecken eines regelmäßigen n-Ecks für gegebenes $n \geq 3$ konstruieren?*

Wir werden beweisen, dass die Antwort auf die beiden Fragen im Allgemeinen 'nein' lautet. Im zweiten Fall lautet die genaue Antwort: dies ist genau dann möglich, wenn $n = 2^k \cdot p_1 \cdot ... \cdot p_k$ für paarweise verschiedene Fermat'sche Primzahlen gilt. Für $n \leq 20$ können genau folgende n-Ecke konstruiert werden:

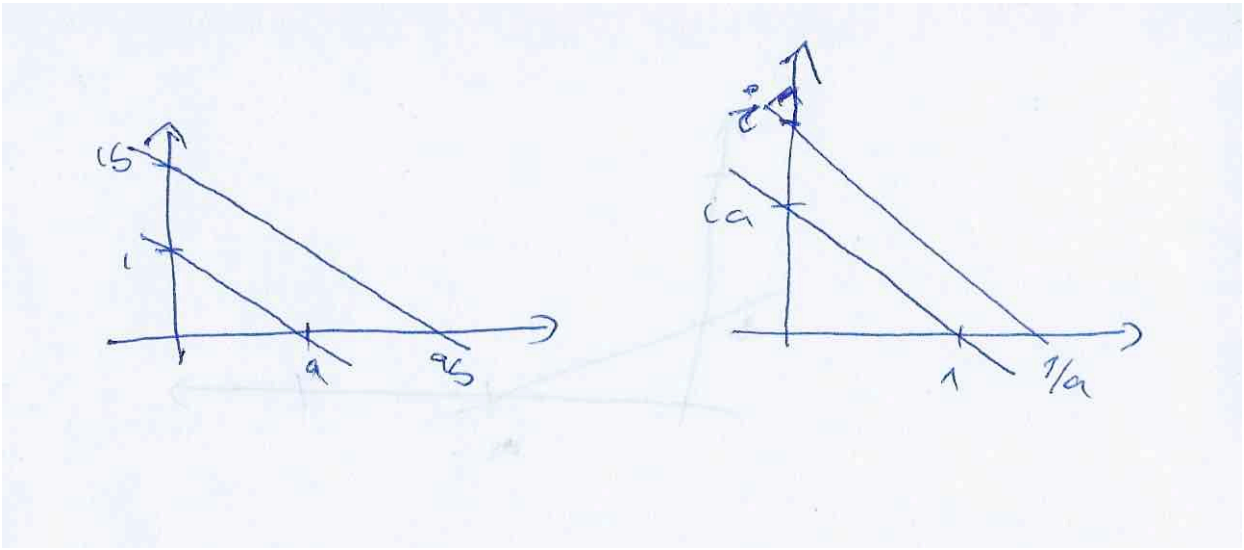
$$3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20$$

Wir wollen nun erklären wie man diese Fragen löst und was sie mit Körpertheorie zu tun hat. Sei $\mathbb{K} \subseteq \mathbb{C}$ die Menge der aus $M = \{0, 1\} \subseteq \mathbb{C}$ konstruierbaren Zahlen.

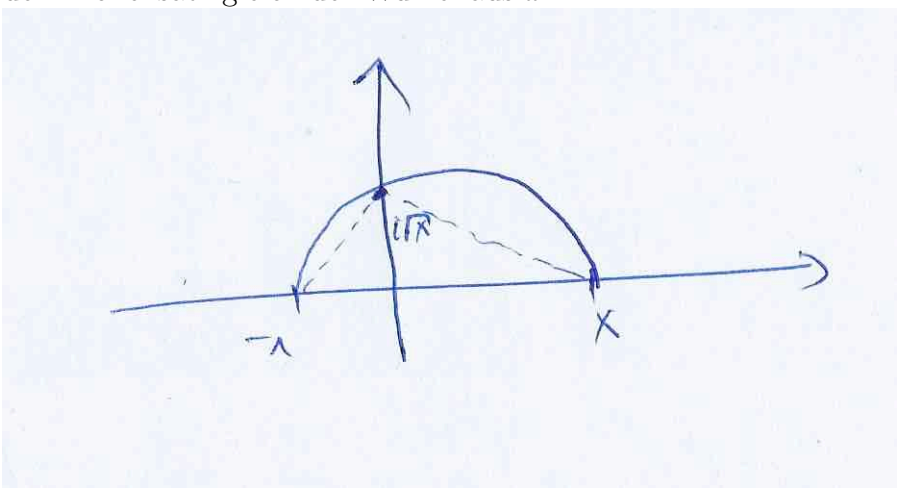
Lemma 2.3. *Es gilt:*

1. *$\mathbb{K}$ ist ein Unterkörper von $\mathbb{C}$, d.h. $0, 1 \in \mathbb{K}$ und für $a, b \in \mathbb{K}$ gilt auch $a + b, ab, -a \in k$ sowie $a^{-1} \in \mathbb{K}$ falls $a \neq 0$.*
2. *$\mathbb{Q} + i\mathbb{Q} \subseteq \mathbb{K}$*
3. *$z \in \mathbb{K} \Leftrightarrow \mathrm{Re}(z), \mathrm{Im}(z) \in \mathbb{K}$*
4. *$\mathbb{K}$ ist quadratisch abgeschlossen, d.h. für $x \in \mathbb{K}$ gilt auch $\pm\sqrt{x} \in \mathbb{K}$.*

Beweis. Nach Definition gilt $0, 1 \in \mathbb{K}$. Damit auch $-1 \in \mathbb{K}$. Daher $i \in \mathbb{K}$ durch Konstruktion der Mittelsenkrechte auf $[-1, 1]$. Dann kann man für eine Zahl $z \in \mathbb{C}$ das Lot auf die Achsen fällen, sodass Realteil $\mathrm{Re}(z)$ und Imaginärteil $\mathrm{Im}(z)$ ebenfalls konstruierbar sind.
Gegeben $a, b \in \mathbb{K}$. Wir konstruieren die Summe als Schnittpunkt zweier Kreise um a und b. Das Inverse $-a$ ensteht durch Punktspiegelung. Jetzt haben wir 2. und 3. bewisen und den ersten Teil von 1. Um das Produkt ab zu konstruieren stellen wir fest, dass sich der Real und Imaginärteil von ab durch die Real- und Imaginärteile von a und b ausdrücken lassen. Also können wir oBdA annehmen, dass a und b reell sind und dann benutzten wir den Strahlensatz: Wir legen eine zu ai Parallele Gerade durch ib sodass der Schnittpunkt mit der x-Achse ab ist. Analog können wir das Inverse einer Zahl $a \in \mathbb{C}^*$ als $a^{-1} = \frac{\overline{a}}{|a|^2}$ darstellen, sodass wir wieder oBdA annehmen können, dass a reell ist und dann können wir wiederum die Parallele Gerade zu $1ia$ durch den Punkt i betrachten:



Damit haben wir auch 1. beweisen. Um 4. zu sehen stellen wir fest, dass man Winkel mit Zirkel und lineal halbieren kann und daher reicht es wegen der Polardastellung von komplexen Zahlen wieder dies für $x \in \mathbb{R}_{\geq 0}$ zu zeigen. Dazu schlagen wir den Thaleskreis über -1 und x. Der Schnittpunkt mit der y-Achse ist dann nach Thales eine rechtwinkeliges Dreieck und daher ist die Höhe nach dem Höhensatz gleich der Wurzel aus x.



□

Definition 2.4. *Sei $K \subseteq E$ eine Körpererweiterung, d.h. K ist ein Unterkörper eines Körpers E und $A \subseteq E$ eine Teilmenge. Wir setzen*

$$K(A) := \bigcap_{A \subseteq F} F$$

wobei der Schnitt über alle Unterkörper $F \subseteq E$ geht, die K und A enthalten.

Dann ist $K(A)$ ein Unterkörper von E (warum?) und offenbar der kleinste Unterkörper der K und A enthält. Wir sagen $K(A)$ ensteht aus K durch adjungieren von A.

Beispiel 2.5. Betrachte Unterkörper von $E = \mathbb{C}$. Dann ist $\mathbb{R}(i) = \mathbb{C}$ und $\mathbb{Q}(i) = \mathbb{Q} + i\mathbb{Q} \subseteq \mathbb{C}$.

Definition 2.6. *Sei E ein Erweiterungskörper E von K*

1. *Wir sagen E entsteht durch* adjungieren einer Quadratwurzel *falls $E = K(x)$ für $x \in E$ mit $x^2 \in K$.*

2. *E ensteht durch sukzessives adjunktieren von Quadratwurzeln wenn es eine Kette*
$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n = E$$
von Unterkörpern gibt sodass K_{i+1} aus K_i durch adjungieren einer Qudratzwurzel entsteht.

Beispiel 2.7. Falls E durch adjungieren einer Quadratwurzel $x \notin K$ ensteht, so gilt
$$E = K + xK = \{a + xb \mid a, b \in K\} \ .$$
Dazu reicht es zu zeigen, dass $K + xK \subseteq E$ ein Unterkörper von E ist. Es gilt
$$\begin{aligned}(a + xb) + (a' + xb') &= (a + a') + x(b + b') \\ -(a + xb) &= -a + x(-b) \\ (a + xb) \cdot (a' + xb') &= (aa' + x^2bb') + x(ab' + a'b) \ .\end{aligned}$$
Somit bleibt es die Existenz von Multiplikativen Inversen zu zeigen. Es gilt für $a, b \in K$ dass $(a + xb)(a - xb) = a^2 - x^2b^2 \in K$ sodass das Inverse von $a + xb$ gegeben ist durch
$$\frac{1}{a + xb} = \frac{a}{a^2 - x^2b^2} - x\frac{b}{a^2 - x^2b^2}$$
falls $a^2 - x^2b^2 \neq 0$. Letztere Gleichung gilt aber immer falls nicht $a = b = 0$, da $a \neq xb$ und $a \neq -xb$ (sonst läge x in K).

Satz 2.8. *Ein Element $z \in \mathbb{C}$ liegt genau dann in $\mathbb{K}$, d.h. ist konstruierbar, wenn z in einem Unterkörper $E \subseteq \mathbb{C}$ liegt der durch sukzessives adjungieren von Quadratwurzeln aus $\mathbb{Q}$ entsteht.*

Beweis. Falls $z \in \mathbb{C}$ in einem Unterkörper E liegt der durch sukzessives adjungieren ensteht, so liegt $z \in \mathbb{K}$ da nach Lemma 2.3 (4) auch Quadratwurzeln darin liegen. Für die Umkehrung reicht es zu zeigen dass für einen gegebenen Unterkörper $M \subseteq \mathbb{C}$ jedes Element $z \in \mathbb{C}$ was durch anwenden eines Konstruktionsschrittes aus M entsteht in einem Quadratischen Erweiterungskörper E' liegt. Wir zeigen dies unter der Annahme, dass M die Eigenschaft hat, dass ein komplexe Zahl z in M liegt genau dann wenn $\mathrm{Re}(z) \in M$ und $\mathrm{Im}(z) \in M$. Der Erweiterungskörper E' erfüllt diese Bedinung dann auch (siehe Übungen) und die Behauptung folgt induktiv (mit Induktonsanfang $M = \mathbb{Q}(i)$).
Der Schnitt zweiter Geraden mit Koeffizienten in $M \cap \mathbb{R}$ (dies ist erfüllt, wenn man die Geraden durch Punkte in M legt...!?) führt auf ein Gleichungssystem welches in M gelöst werden kann:
$$(x, ax + b) = (x', a'x' + b') \Rightarrow x = x' = \frac{b' - b}{a - a'} \ .$$
Ein Kreis mit Radius und Mittelpunkt in M kann durch die Menge aller Punkte $(x, y) \in \mathbb{R}^2 = \mathbb{C}$ mit
$$(x - a)^2 + (y - b)^2 = r^2$$

für $a, b, r \in M \cap \mathbb{R}$ beschrieben werden. Der Schnitt einer Gerade mit einem Kreis, oder der Schnitt zweiter Kreise führt auf eine quadratische Gleichung mit Koeffizienten in M, deren Lösungen mittels einer Wurzel eines Elementes aus M ausgedrückt werden kann, also in einem quadratischen Erweiterungskörper liegt. □

Definition 2.9. *Seit $K \subseteq E$ eine Körpererweiterung. Durch Einschränken der Multiplikation $E \times E \to E$ zu einer Abbildung $K \times E \to E$ betrachten wir E als Vektorraum über K. Dann ist*

$$[E : K] := \dim_K(E)$$

der Grad der Körpererweiterung (dieser kann endlich oder unendlich sein).

Beispiel 2.10. Es gilt $[\mathbb{C} : \mathbb{R}] = 2$ und $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ aber $[\mathbb{R} : \mathbb{Q}] = \infty$. Letzteres weil $\mathbb{R}$ überabzählbar und $\mathbb{Q}$ abzählbar ist. Falls E durch adungieren einer Wurzel aus K entsteht gilt $[E : K] = 2$, siehe Beispiel 2.7.

Es gilt auch die Umkehrung des letzten Beispieles.

Lemma 2.11. *Sei* $\mathrm{char}(K) \neq 2$*, d.h.* $1 + 1 \neq 0$ *in K und $[E : K] = 2$. Dann ensteht E durch adjungieren einer Wurzel.*

Beweis. Sei $x \in E \setminus K$. Dann bildet $1, x$ eine Basis von E über K und es gilt $E = K(x)$. Es gilt also auch $x^2 = ax + b$ für $a, b \in K$. Wir setzen $x' := x + a/2$. Es gilt $K(x') = K(x) = E$ und ausserdem

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

□

Bemerkung 2.12. Falls $\mathrm{char}(K) = 2$ so ist immernoch jede Erweiterung mit $[E : K] = 2$ von einem Element erzeugt, welches eine quadratische Gleichung über K erfüllt, aber es muss keine Wurzel sein. Zum Beispiel ist $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ aber für $x \in \mathbb{F}_4$ gilt $x^2 \in \mathbb{F}_2$ genau dann wenn $x \in \mathbb{F}_2$. Tatsächlich gilt für $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$ die Gleichung $x^2 + x + 1 = 0$.

Satz 2.13 (Gradformel)**.** *Für einen Turm $K \subseteq F \subseteq E$ von Körpererweiterungen gilt*

$$[E : K] = [E : F] \cdot [F : K]$$

Beweis. Durch Basiswahl von E als F-Vektorraum bekommen wir einen Isomorphismus von F-Vektorräumen $E \cong \bigoplus_{j \in J} F$. Dies ist dann auch ein Isomorphimus von K-Vektorräumen. Eine Basiswahl von F über K liefert einen Isomorphimus von K-VR $F \cong \bigoplus_{i \in I} K$. Dann gilt

$$E \cong \bigoplus_{j \in J} F \cong \bigoplus_{i,j \in I \times J} K$$

als K-Vektorräume. □

Korollar 2.14. *Für ein konstruierbares Element $z \in \mathbb{C}$ gilt*

$$[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$$

mit $n \in \mathbb{N}$.

Beweis. Es folgt aus Satz 2.8 dass z in einem Unterkörper $E \subseteq \mathbb{C}$ liegt der durch sukzessives adjungieren von Quadratwurzeln ensteht. Dann gilt aber nach der Gradformel, dass $[E : \mathbb{Q}] = 2^k$. Der Körper $\mathbb{Q}(z) \subseteq E$ ist dann ein Unterkörper, muss dann aber nach der Gradformel als Dimension einen Teiler von 2^k haben. □

3 Algebraische Körpererweiterungen

Wir haben bisher Lösungen von quadratischen Gleichungen (d.h. Wurzeln) adjungiert. Nun wollen wir beliebige Polynome zulassen.
Wir erinnern an die Definition des Polynomringes $K[X]$ dessen Elemente Polynome über K in einer Veränderlichen X sind. [1] Für eine Körpererweiterung $K \subseteq E$ können wir ein solches auch als Polynom in E auffassen, was wir implizit tun werden.

Definition 3.1. *Sei E/K eine Körpererweiterung. Ein element $\alpha \in E$ heisst algebraisch über K falls es ein Polynom $0 \neq p \in K[x]$ gibt mit $p(\alpha) = 0$. Anderenfalls heisst α transzendent.*

Bemerkung 3.2. Man kann oBdA annehmen, dass der Leitkoeffizient von p eins ist, d.h.

$$p = x^n + a_{n-1}x^{n-1} + ... + a_0 \ .$$

Für die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{C}$ spricht man einfach von transzendenten und algebraischen Zahlen. Es ist ein Satz von Lindemann (1882), dass π transzendent (über $\mathbb{Q}$ ist). Die Eulersche Zahl e ist ebenfalls transzendent.

Satz 3.3. *Sei E/K eine Körpererweiterung. Dann ist x genau dann algebraisch über K falls $[K(\alpha) : K] < \infty$.*

Beweis. Sei $[K(\alpha) : K] < \infty$. Dann können die Elemente $1, \alpha, \alpha^2, ...$ nicht linear unabhängig sin und es muss eine Relation

$$\sum_{i=0}^{n} a_n \alpha^n = 0$$

geben, was zeigt, dass α algebraisch ist.
Umgekehrt sei α algebraisch. Wir betrachten die Menge $K[\alpha] \subseteq E$ bestehend aus allen Elementen die sich als Polynome in α ausdrücken lassen. Die ist offensichtlich ein Unterring von E und als K-Vekorraum hat er endliche Dimensi

[1] Wir erinnern daran, dass ein Ring eine Menge R mit Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ sowie Elementen $0, 1 \in R$ is, sodass $(R, +, 0)$ eine abelsche Gruppe ist, $(R, \cdot, 1)$ eine Monoid ist und die Distributivgesetze gelten.

da eine $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ ein Erzeugendensystem ist (nach Annahme lässt sich α^n als Linearkombination schrieben wobei n der Grad des Polynoms ist. Wir betrachten die K-linear Abbildung

$$- \cdot x : K[\alpha] \to K[\alpha]$$

gegeben durch Multiplikation mit einem Element $x \in K[\alpha]$. Diest ist injektiv, da x ein Inverses in E hat. Also ist sie auch surjektiv. Insbesondere existiert $y \in K[\alpha]$ mit $yx = 1$. Es folgt, dass $K[a]$ ein Körper ist und somit $K[a] = K(\alpha)$. □

Korollar 3.4. *Jede konstruierbare Zahl $z \in \mathbb{C}$ ist algebraisch über $\mathbb{C}$. Insbesondere ist weder π noch $\sqrt{\pi}$ konstruierbar und daher die Quadratur des Kreises unmöglich.*

Wir erinnern an den Begriff des Minimalpolynoms einer K-linearen Abbildung $A : V \to V$ aus der linearen Algebra. Dies ist das normierte Polynom minimalen Grades $p \in K[x]$ sodas $p(A) = 0$ in dem Ring der Endomorphismen $\mathrm{End}_K(V)$. Hierbei haben wir den Einsetzungshomomorphismus

$$K[x] \to \mathrm{End}_K(V)$$

verwendet, welcher x auf A sendet, und ein Homomorphimus von unitalen Ringen ist (d.h. Ringe mit 1). Beachte, dass $\mathrm{End}_K(V)$ ein nicht-kommutativer Ring ist.

Definition 3.5. *Sei $\alpha \in E$ algebraisch über $K \subseteq E$. Dann ist das Minimalpolynom $\min_K(\alpha) \in K[x]$ von α über K das Minimalpolynom der linearen Abbildung*

$$L_\alpha : K(\alpha) \to K(\alpha) \qquad x \mapsto \alpha x$$

Äquivalent lässt sich $\min_K(\alpha)$ als das eindeutige normierte Polynom minimalen Grades beschrieben welches α als Nullstelle hat, denn für ein Polynom $p \in K[x]$ gilt in $\mathrm{End}_K(K(\alpha))$ die Gleichung $p(L_\alpha) = L_{p(\alpha)}$ und $L_{p(\alpha)} = 0$ genau dann wenn $p(\alpha) = 0$.

Satz 3.6. *Es gilt $[K(\alpha) : K] = \deg \min_K(\alpha)$.*

Proof. Sei $n = \deg \min_K(\alpha)$. Wir sehen, dass $1, x, x^2, ..., x^{n-1}$ ein Erzeugendensytem von $K(\alpha) : K$ ist (wir erinnern, dass $K(\alpha) = K[\alpha]$). Angenommen es wäre linear abhängig, so gäbe es eine Linearkombination

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + ... + a_0 \cdot 1 = 0 \ .$$

Dies wäre aber dann ein Polynom mit α als Nullstelle im Widerspruch zur Minimalität des Minimalpolynoms. □

Beispiel 3.7. Wir betrachten die Körpererweiterung

$$\mathbb{Q}(\zeta_3)/\mathbb{Q}$$

wobei $\zeta_3 = \exp(2\pi/3)$ eine primitive dritte Einheitswurzel ist. Es gilt die Gleichung

$$0 = \zeta_3^3 - 1 = (\zeta_3 - 1)(\zeta_3^2 + \zeta_3 + 1)$$

Also $\zeta_3^2 + \zeta_3 + 1 = 0$. Wir behaupten, dass $1 + x + x^2$ das Minimalpolynom von ζ_3 über $\mathbb{Q}$ ist. Anderenfalls müsste das Minimalpolynom Grad 1 haben und damit $\zeta_3 \in \mathbb{Q}$ liegen. Es folgt, dass $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ und daher eine quadratische Erweiterung bildet. Wir schließen, dass ζ_3 und damit das reguläre Dreick konstruierbar ist (das wussten wir natürlich auch bereits geometrisch).

Bemerkung 3.8. Sei $\zeta_n = \exp(2\pi i/n)$. Wir haben gesehen, dass es für die Konstruktion des regelmäßigen n-Ecks notwendig ist, dass

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k.$$

Es muss also die Bedingung erfüllt sein, dass das Minimalpolynom von ζ_n als Grad eine Zweierpotenz hat. Damit kann man tatsächlich schon auf die gegebenen Antwort kommen, z.B. das das regelmäßige 7-Eck nicht konstruierbar ist. Wir werden sehen, dass dies in diesem Fall auch hinreichend ist (mittels Galois Theorie).

Definition 3.9. *Eine Körpererweiterung E/K heisst algebraisch, falls jedes Element algebraisch ist.*

Korollar 3.10. *Jede endlich Körpererweiterung (d.h. $[E : K] < \infty$) ist algebraisch und der Grad des Minimalpolynoms jedes Elemetes teilt den Körpergrad.*

Die Umkehrung gilt nicht, es gibt algebraische Körpererweiterungen die nicht endlich sind, zum Beispiel $\mathbb{K}/\mathbb{Q}$.

Satz 3.11. *Sei E/K eine Körpererweiterung sodass $E = K(M)$ für eine Menge M von über K algebraischen Elementen. Dann ist E algebraisch.*

Proof. Es gilt zunächst, dass

$$K(M) = \bigcup_{M_0 \subseteq M} K(M_0)$$

wobei M_0 durch alle endlichen Teilmengen läuft. dies folgt daraus, dass die Vereiningung offensichtlich ein Unterkörper ist und M enthält. Damit können wir oBdA annehmen, dass M endlich ist. Für endliches $M = \{\alpha_1, ..., \alpha_n\}$ ist

$$K(M) = K(\alpha_1)(\alpha_2)...(\alpha_n)$$

und jedes Element α_i ist algebraisch über dem Körper $K(\{\alpha_1, ..., \alpha_{i-1})$ da es algebraisch über K ist. Aus der Gradformel folgt, dass $[K(M) : K] < \infty$ und die Behauptung. □

Korollar 3.12. *Für eine Körpererweiteung $K \subseteq E$ betrachten wir die Menge $F \subseteq E$ aller algebraischen Elemente über K. Dies ist der maximale algebraischer Unterkörper von E der K enthält.*

Proof. Um zu sehen, dass es ein Zwischenkörper ist, stellen wir fest, dass für $a, b \in F$ auch $K(a, b)$ Teilmenge von F ist (da alle Elemente algebraisch sind). Also sind auch Produkt, Summe etc enthalten. Weiterhin ist F offensichtlich algebraisch. □

Korollar 3.13. *Für einen Turm von Körpererweiterungen $K \subseteq F \subseteq E$ gilt, dass E/K algebraisch ist genau dann wenn F/K und E/F algebraisch sind.*

Proof. Falls E/K algebraisch ist, so sind offensichtlich auch F/K und E/F algebraisch (wir können jeweils für jedes Element entsprechende Polynome finden). Umgekehrt seien F/K und E/F algebraisch und $e \in E$ gebeben. Betrachte eine Polynom

$$p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in F[x]$$

welches e anhiliert. Dann ist e algebraisch über $K(a_0, .., a_{n-1})$ und daher

$$[K(a_0, .., a_{n-1})(e) : K(a_0, .., a_{n-1})] < \infty$$

und deswegen wegen der Gradformel auch endlich über K (weil alle a_i algebraisch sind). Das zeigt, dass e auch algebraisch über K ist. □

Beispiel 3.14. Die Menge der rationalen Zahlen

$$\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ algebraisch über } \mathbb{Q}\} \subseteq \mathbb{C}$$

ist eine algebraische Körpererweiterung von $\mathbb{Q}$. Die Menge der Konstruierbaren Zahlen ist ein Unterkörper $\mathbb{K} \subseteq \overline{\mathbb{Q}}$ und die Inklusion ist echt. Beide diese Erweiterungen sind unendlich.

4 Ideale in Ringen

Wir erinnern nochmal and die Begriffe Ring, Ringhomomorphismus (immer mit 1) und Unterring. In diesem Kapitel wollen wir einige Begriffe für Ringe einführen. Wir empfehlen als Standardbeispiele stets $\mathbb{Z}$ und $K[x]$ im Kopf zu behalten. Das Hauptziel der kommenden Vorlesungen wird es sein, Methoden zu lernen um Minimalpolynome von Elementen in Körpererweiterungen zu bestimmen, zum Beispiel für die Einheitswurzel ζ_n über $\mathbb{Q}$.

Definition 4.1. *Sei R ein Ring. Ein (beidseitiges) Ideal ist eine Teilmenge $I \subseteq R$ sodass I eine Untergruppe bezüglich addition ist und sodass für $i \in I$ und $r \in R$ gilt $ri, ir \in I$.*

Beispiel 4.2.

1. Für jeden Ring ist $\{0\} \subseteq R$ ein Ideal (das Nullideal). Wir schreiben auch 0 dafür.

2. Falls für ein Ideal $1 \in I$ gilt so folgt bereits $I = R$. Allgmeiner, wenn ein Ideal I ein invertierbares Element $r \in R^\times$ enthält, so folgt bereits, dass $1 = r^{-1}r \in I = R$. Insbesondere sind für einen Körper K die einzigen Ideal $\{0\}, K$.

3. Für jeden kommutativem Ring R und jedes Element $r \in R$ existiert das Ideale
$$(r) = rR = \{xr \mid x \in R\} \subseteq R$$
gennant das von r erzeugte Hauptideal. Es besteht aus allen Vielfachen von r (auch durch r teilbare Elemente genannt). Für nicht kommutative Ringe sieht das von $r \in R$ erzeugte Ideal $(r) \subseteq R$ etwas komplizierter aus (wie?).

4. Jedes Ideal $I \subseteq \mathbb{Z}$ hat die Form $n\mathbb{Z} \subseteq \mathbb{Z}$ für ein eindeutig bestimmtes $n \in \mathbb{N}$. Dazu sei $I \subseteq \mathbb{Z}$ ein Ideal. Wähle ein minimales Element n in $I \cap \mathbb{N}$. Dann ist $n\mathbb{Z} \subseteq I$. Falls ein $i \in I$ existiert mit $i \neq n\mathbb{Z}$ so können wir obda annehmen, dass $i > 0$. Durch division mit Rest schreiben wir $i = i_0 + ni_1$ mit $0 < i_0 < n$ und $i_1 \in \mathbb{N}$. Es folgt $i_0 \in I$ im Widerspruch zu Minimalität von n.

5. Genauso sehen wir, dass alle Ideal in $K[x]$ Hauptideale sind: sei $p \in I$ normiert von minimalen Grad. Dann folgt durch Widerspruch und Division mit Rest, dass $I = (p)$ gilt. Wenn man das Polynom normiert ist es eindeutig durch das Ideal bestimmt.

6. Für jede Teilmenge $M \subseteq R$ von Elementen gibt es das von M erzeugte Ideal
$$(M) = \bigcap_{I \supset M} I$$
wobei der Schnitt über alle Ideale $I \subseteq R$ geht, die M enthalten. Konkret besteht dieses Ideal für kommutative Ring R aus allen endlichen Linearkombinationen von Elementen in M. Auf diese Art haben wir auch Ideale $(a_1, .., a_n) \subseteq R$ für endlich viele Elemente $a_1, ..., a_n$.

7. Für jeden Ringhomomorphismus $f : R \to S$ ist der Kern
$$\ker(f) = \{r \in R \mid f(r) = 0\}$$
ein Ideal in R. Allgemeiner ist für ein Ideal $I \subseteq S$ das Urbild $f^{-1}(I)$ ein Ideal in R wie man sofort anhand der Definition sieht.

8. Für jedes Paar $I, J \subseteq R$ von Idealen ist auch
$$I + J = \{i + j \mid i \in I, j \in J\} \subseteq R$$
ein Ideal.

9. Das Produkt Ideal ist
$$I \cdot J = \{i_1 j_1 + ... + i_n j_n \mid i_k \in I, j_k \in J\} = (ij \mid i \in I, j \in J) \ .$$

Definition 4.3. *Für ein Ideal $I \subseteq R$ definieren wir den Quotientenring R/I wie folgt: die unterliegende Menge ist die Menge der Äquivalenzklassen $R/\sim$ wobei*
$$x \sim y \Leftrightarrow x - y \in I \ .$$

(Dies ist offensichtlich eine Äquivalenzrelation wie man sofort nachrechnet). Dies wird ein Ring indem wir definieren

$$[r] + [s] = [r + s] \qquad 0 = [0] \qquad [r] \cdot [s] = [rs] \qquad 1 = [1]$$

Um zu sehen, dass die letzte Definition wohldefiniert ist muss man zeigen, dass die Wahl der Addition und Multiplikation wohldefiniert ist, d.h. nicht von der Wahl der Representanten r, s abhängt. Dies überlassen wir dem Leser.
Per Definition ist die Abbildung

$$\pi : R \to R/I \qquad r \mapsto [r]$$

ein Homomorphismus von Ringen. Der Kern dieses Homomorphismus ist offensichtlich I. Wir haben damit gezeigt, dass jedes Ideal I als Kern eines Ringhomomorphismus ensteht.

Beispiel 4.4. Die Ringe $\mathbb{Z}/n\mathbb{Z}$ sind Quotientenringe. Wir schreiben diese auch als $\mathbb{Z}/n$. Für jeden Ring R und $r \in R$ können wir den Quotienten R/rR bilden. Wir schreiben dies auch als R/r.

Beispiel 4.5. Für ein Polynom $0 \neq p \in K[x]$ von Grad n gibt es den Ring $K[x]/p$. Dieser Ring enthält K als konstante Polynome, denn die Abbildiung $K \to K[x]/p$ ist injektiv. Wir können damit $R[x]/p$ als K-Vektorraum auffassen. Er ist als K-Vektorraum erzeugt von $1, x, x^2, ..., x^{n-1}$, da in disem Quotienten gilt

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 = 0 \ .$$

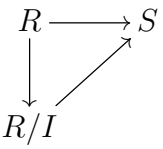
Es lässt sich also x^n als Linearkombination der Basis darstellen. Ähnlliches gilt für die höheren x^i. Ausserdem sind die $x_1, .., x_{n-1}$ linear unabhängig. Anderenfalls müsste es eine Linearkombination

$$b_0 + b_1 x + ... + b_{n-1} x^{n-1}$$

geben die in $K[x]/p$ verschwindet, also müsste die gleiche Linearkombination in $K[x]$ ein Vielfaches von p liefern. Das ist aber aus Gradgründen unmöglich.

Beispiel 4.6. Die Ideale des Ringes R/I stehen in Bijektion zu den Idealen von R welche I enthalten (Übung!). Insbesondere sind die Ideale von $\mathbb{Z}/n$ gegeben durch die Teiler von n. Die Ideale in $R[x]/p$ sind gegeben durch die normierten Teiler von p.

Satz 4.7 (Universelle Eigenschaft)**.** *Für jeden Ringhomomorphimus $\varphi : R \to S$ mit $\varphi(I) = 0$ existiert ein eindeutiger Homomorphismus $\varphi' : R/I \to S$ sodass das Diagram*



kommutiert. Falls $R \to S$ surjektiv ist und $I = \ker(\varphi)$ so ist diese Abbildung ein Isomorphismus.

Proof. dd □

Die universelle Eigenschaft legt den Quotienten eindeutig fest (warum?). Eine andere Art die universelle Eigenschaft zu schreiben ist zu sagen, dass postcompositon mit $R \to R/I$ eine Bijektion

$$\mathrm{Hom}_{\mathrm{Ring}}(R/I, S) = \{\varphi : R \to S\} \xrightarrow{\simeq} \{\varphi : R \to S \mid \varphi(I) = 0\}$$

induziert.

Beispiel 4.8. Betrachte eine Körpererweiterung E/K und $\alpha \in E$. Dann ist der Einsetzungshomomorphimus $K[x] \to E$ surjektiv auf den Unterring $K[\alpha] \subseteq E$. Der Kern ist das Verschwindungsideal I von α, d.h. die Menge aller Polynome p sodass $p(\alpha) = 0$. Dann ist

$$K[x]/I \to K[\alpha]$$

ein Isomorphismus. Es gilt aber nun entweder $I = 0$ (wenn α transzendent über K ist). In dem Fall ist

$$K[\alpha] \cong K[x]$$

oder es gilt $I = (p)$ wenn α algebraisch ist. Dann ist p das Minimalpolynom von α und es folgt

$$K[x]/p = K[\alpha] = K(\alpha).$$

Wir sehen auch, dass jedes weitere Polynom $p \in K[x]$ welches α annihiliert von dem Minimalpolynom geteilt wird.

Allgemein kann man sich fragen, für welche Polynome p der Quotient $K[x]/p$ wieder ein Körper ist. Offensichtlich ist dies nach dem letzten Beispiel für Minimalpolynome von algebraischen Elementen in E der Fall und wir werden im kommenden Kapitel sehen wie man das im Allgemeinen entscheidet.

5 Integritäts- und Hauptidealringe

Definition 5.1. *1. Ein kommutativer Ring heisst Integritätsring (oder Nullteilerfrei), falls er keine Nullteiler bestitzt, d.h. falls aus $xy = 0$ folgt $x = 0$ oder $y = 0$ (äquivalent: Multiplikation $L_x : R \to R$ für $x \neq 0$ ist injektiv).*

2. Ein Integritätsring heisst Hauptidealring (engl. PID, principal ideal domain), wenn jedes Ideal ein Hauptideal ist, das heisst von der Form (r) für $r \in R$ ist.

Beispiel 5.2. 1. Alle Körper sind Integritätsringe und sogar Hauptideal Ringe.

2. Die Ringe $\mathbb{Z}$ und $K[x]$ sind ebenfalls Hauptidealringe (K wie immer ein Körper). Wir haben bereits gesehen, dass alle Ideal Prinzipal sind.

3. Man kann die Division mit Rest die es in $\mathbb{Z}$ und $K[x]$ gibt auch formalisieren: ein Integritätsring heißt *euklidischer Ring*, wenn es eine Abbildung

$$\deg : R \setminus \{0\} \to \mathbb{N}$$

gibt, so dass es zu $a, b \in R$ mit $a \neq 0$ Elemente $q, r \in R$ gibt so dass $b = qa + r$ gilt und $r = 0$ oder $\deg(r) < \deg(a)$. Beispiele sind $\mathbb{Z}$ mit $\deg(-) = |-|$ und der Polynomring mit Bewertungsfunktion gegeben durch den Grad des Polynoms.

Es folgt mit dem Gleichen Argument wie für $\mathbb{Z}$ und $K[x]$, dass jeder euklidische Ring ein Hauptidealring ist: jedes Ideal I muss ein Element $r \neq 0$ minimalen Grades enthalten. Für eine beliebiges element $i \in I$ gilt dann, dass $i = ra$ da ansonsten Division mit Rest eine Element kleineren Grades in I liefern würde.

4. Betrachte für einen beliebigen Ring R die Menge $R \times R$ mit Komponentenweise Addition und Multiplikation, d.h.

$$(a, b) + (a', b') = (a + a', b + b') \qquad (a, b) \cdot (a', b') = (aa', bb')$$

Dies ist offenbar ein Ring, der kommutativ ist, falls R kommutativ ist. Das Nullelement ist $(0, 0)$. Es gilt $(1, 0) \cdot (0, 1) = (0, 0)$. Also ist $R \times R$ nicht Nullteilerfrei.

5. Der Ring $\mathbb{Z}/n$ für $n \neq 0$ ist genau dann Nullteilerfrei, weil die Abbildung

$$\cdot k : \mathbb{Z}/n \to \mathbb{Z}/n$$

genau dann injektiv ist, wenn sie Surjektiv ist (aufgrund der Endlichkeit von $\mathbb{Z}/n$). Dies ist der Fall für n eine Primzahl. Wir schreiben $\mathbb{Z}/p$ auch als $\mathbb{F}_p$.

Zum Beispiel gilt in $\mathbb{Z}/ab$ die Relation $ab = 0$ aber $a \neq 0$ und $b \neq 0$.

6. Für jeden Integritätsring R können wir den Quotientenkörper $Q(R)$ bilden und dieser enthält $R \subseteq Q(R)$. Umgekehrt ist jeder Unterring eines Körpers offensichtlich ein Integritätsring. Es folgt also, dass Integritätsringe genau die Unterringe von Körpern sind.

7. Für jeden Nullteilerfreien Ring R ist auch der Polynomring $R[x]$ Nullteilerfrei. Dazu betrachte einfach die Leitkoeffizienten.

8. Betrachte in dem Polynomring $\mathbb{Z}[x]$ die Menge aller Polynome $p \in \mathbb{Z}[x]$ deren Absolutglied durch 2 teilbar ist, d.h.

$$I = \{a_n x^n + ... + a_0 \mid a_0 \in 2\mathbb{Z}\} = (x, 2)$$

Falls I ein Hauptideal wäre, so müsste es von der Form (p) sein, also müsste sowohl 2 als auch x ein Vielfaches von p sein. Die einzigen Elemente die das konstante Polynom 2 teilen sind aber ± 1 und ± 2. Nur ± 1 teilt auch x. Aber das davon erzeugte Ideal ist $\mathbb{Z}[x]$. Insbesondere kann $\mathbb{Z}[x]$ auch kein Euklidischer Ring sein (gute Übung).

Tatsächlich haben wir:

Satz 5.3. *Sei R ein kommutativer Ring. Dann ist $R[x]$ ein Hauptidealring genau dann wenn R ein Körper ist.*

Proof. Wir haben bereits gesehen, dass für einen Körper $R = K$ der Ring $K[x]$ ein Hauptidealring ist.
Sei also umgekehrt $R[x]$ ein Hauptidealring. Insbesondere ist $R[x]$ Nullteilerfrei. Dann ist auch R Nullteilerfrei, denn falls $ab = 0$ in R so können wir diese Gleichung in $R[x]$ interpretieren und bekommen, dass $a = 0$ oder $b = 0$ (in $R[x]$ also in R). Sie $I \neq 0$ ein Ideal in R. Wir betrachten das Ideal

$$(x) + (I) = \{xp(x) + iq(x) \mid i \in I, p(x), q(x) \in R[x]\}$$

Wäre dies von p erzeugt, so müsste p ein Teiler von x sein, also $p = \pm 1$. Dann folgt aber, dass das Ideal bereits ganz $R[x]$ wäre, also insbesondere $I = R$.
Wir haben also gezeigt, dass jedes nicht-triviale Ideal I in R bereits R ist. Dann ist R aber ein Körper, denn wenn $1 \in (r)$ so muss s existieren, sodass $rs = 1$. □

Bemerkung 5.4. Sei R ein Hauptidealring. Dann existiert zu beliebig vorgegebenen $a, b \in R$ ein größter gemeinsamer Teiler $d \in R$, d.h ein Element welches a und b teilt (im offensichtlichen Sinne) und sodass jedes weitere Element welches a und b teilt auch d teilt. Weiterhin gibt es Elemente $r, s \in R$ sodass

$$d = ra + sb \qquad \text{(Lemma von Bézout)}$$

Bevor wir die Existenz von d beweisen, stellen wir zunächst fest, dass die Schreibweise nach dem Lemma bereits die Minimalität impliziert: denn falls $d = ra + sb$ gilt, so teilt jeder Teiler von a und b auch d.
Ausserdem stellen wir fest, dass die Minimalität d schon fast eindeutig festlegt: gegeben d und d' welche ggTs im obigen Sinne sind. Dann folgt dass $d|d'$ und $d'|d$. Das bedeutet aber, dass $d' = xd$ und $d = yd'$. Damit folgt aber $xyd = d$ was wegen der Integrität impliziert, dass $xy = 1$. Daher unterscheiden sich d und d' um eine Einheit.
Nun zum Beweis: wir schreiben das Ideal (a, b) als (d) und bekommen die obige Bézout-Beschreibung von d automatisch. Ausserdem teil d die Elemente a und b, da beide in (a, b) liegen.
Upshot: $(a, b) = (ggt(a, b))$.

Beispiel 5.5. In $\mathbb{Z}$ liefert dies den klassischen ggT. Im Polynomring bekommen wir auf diese Art und Weise auch einen größten gemeinsamen Teiler. Allgmein kann man in euklidischen Ringen mittels Division mit Rest den ggT bestimmen, indem man einen Erzeuger des Ideals (a, b) mittels des erweiterten euklidischen Algorithmus findet:

1. Ordne a und b sodass $\deg(b) \leq \deg(a)$.
2. Schreibe $a = xb + c$ mit $\deg(c) < \deg(b)$. Dann ist

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

3. Durch iterieren dieses Schrittes terminiert der Algorithmus, d.h. das kleinere Element wird 0 und man ist fertig.

Definition 5.6. *Zwei Ideale I und J in einem Ring R heissen teilerfremd, falls $I + J = R$ gilt.*

Beispiel 5.7. 1. Für $R = \mathbb{Z}$ gilt. dass (a) und (b) teilfremd genau dann, wenn a und b teilerfremd sind. Aus letzterem folgt, dass $1 = xa + yb$ und daher $\mathbb{Z} = (a) + (b)$. Andersum lässt sich 1 als Summe von a und b schreiben und es folgt, dass a und b teilerfremd sind (da 1 der ggT ist).

2. Allgmeiner gilt in einem Hauptidealring R, dass $(a) + (b) = R$ genau dann, wenn a und b teilerfremd sind.

Lemma 5.8. *1. Seien I und J teilfremde Ideale. Dann gilt*

$$I \cdot J = I \cap J$$

2. Falls I teilfremd zu $J_1, ..., J_n$ ist, so ist auch I auch teifremd zum Produkt $J_1 \cdot ... \cdot J_n$.

Proof. Dazu machen wir uns klar, dass $I \cdot J \subseteq I \cap J$ immer gilt. Wir müssen also die umgekehrte Inklusion zeigen. Dazu schreiben wir $1 = i + j$. Dann ist ein beliebiges Element $r \in I \cap J$

$$r = 1r = ir + jr \in I \cdot J.$$

Zu (2): Sei $1 = i_k + j_k$ für jedes $k = 1, 2, .., n$. Wir Multiplizieren diese Gleichungen und erhalten

$$1 = i_1 i_2 ... i_k + ... + j_1 \cdot ... \cdot j_k$$

Alle Summenden bis auf den letzten liegen in I. Also haben wir eine Darstellung

$$1 = i + j$$

mit $i \in I$ und $j \in \prod J_k$ gefunden. □

Satz 5.9 (Chinesischer Restsatz)**.** *Sei R ein beliebiger kommutativer Ring und $I_1, .., I_n$ Ideale die paarweise teilerfremd sind. Dann ist die Abbildung*

$$\begin{aligned} R/(I_1 \cdot ... \cdot I_n) &\to R/I_1 \times R/I_2 \times ... \times R/I_n \\ [x] &\mapsto ([x], ..., [x]) \end{aligned}$$

ein Isomorphismus von Ringen. Hierbei trägt die rechte Seite die komponentenweise Addition und Multiplikation.

Proof. Wir behandeln zunächst den Fall $n = 2$. Wir betrachten also die Abbildung

$$R/(I_1 I_2) \to R/I_1 \times R_{I_2}$$

Der Kern dieser Abbildung ist $I_1 \cap I_2$ welches gleich $I_1 I_2$ ist (nach Lemma 5.8). Wir müssen also zeigen, dass die Abbildung surjektiv ist. Dazu sei $1 = i_1 + i_2$. Für ein Element $[r_1] \in R/I_1$ und $[r_2] \in R/I_2$ betrachte

$$r := i_1 r_2 + i_2 r_1.$$

Wir behaupten, dass dies ein Urbild ist, denn

$$r \mod I_1 = i_2 r_1 \mod I_1 = (1 - i_1) r_1 \mod I_1 = r_1 \mod I_1$$

und umgekehrt. □

Beispiel 5.10. Für verschiedene Primzahlen p, q gilt:

$$\mathbb{Z}/pq = \mathbb{Z}/p \times \mathbb{Z}/q \ .$$

Sie $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{k_1} \cdot ... \cdot p_s^{k_2}$ mit paarweise verschiednen Primzahlen. Dann gilt

$$\mathbb{Z}/n = \mathbb{Z}/p_1^{k_1} \times ... \times \mathbb{Z}/p_s^{k_2} \ .$$

Beispiel 5.11. Sei $p = p_1 p_2 \in K[x]$ mit teilerfremden Polynomen p_1 und p_2. Dann gilt

$$K[x]/p = K[x]/p_1 \times K[x]/p_2 \ .$$

6 Primfaktorzerlegung

Definition 6.1. *Sei R ein kommutativer Ring (wie immer mit 1). Ein Ideal $I \neq R$ heisst Primideal, wenn R/I ein Integritätsring ist. Dies ist äquivalent dazu, dass*

$$ab \in I \Rightarrow a \in I \text{ oder } b \in I$$

gilt (warum?).
Ein Ideal $I \neq R$ heisst maximales Ideal, falls R/I ein Körper ist. Dies ist äquivalent dazu, dass jedes Ideal I' mit $I \subsetneq I'$ gilt $I' = R$, daher der Name.

Beispiel 6.2.

1. Ein kommutativer Ring ist genau dann ein Integritätsring, wenn (0) ein Primideal ist.
2. Jedes maximal Ideal ist ein Primideal (denn Körper sind Integritätsringe).
3. In $\mathbb{Z}$ ist ein Ideal $I = n\mathbb{Z} \subseteq \mathbb{Z}$ genau dann prim, wenn n eine Primzahl ist oder wenn $n = 0$. Die maximalen Ideale sind genau die Ideale der Form $p\mathbb{Z}$ mit p prim (also alle Primideale bis auf (0)).

Definition 6.3. *Sei R ein Integritätsring.* [2] *Ein Element $\pi \in R$ heisst irreduzibel (oder unzerlegbar) wenn $\pi \neq 0$ und $\pi \notin R^\times$ und wenn $ab = r$ impliziert, dass entweder $a \in R^\times$ oder $b \in R^\times$.*
Ein Element $\pi \in R$ heißt Primelement, falls $\pi \neq 0$ keine Einheit ist und $\pi | ab$ impliziert, dass $\pi | a$ oder $\pi | b$.

[2] Man konnte diese Forderung hier auch fallen lassen, aber wir wollen uns sowieso auf den Fall von Integritatsringen beschranken

Bemerkung 6.4. 1. Ein Element $\pi \neq 0$ ist genau dann prim, wenn $(\pi) \subseteq R$ ein Primideal ist, denn $ab \in (\pi)$ bedeutet genau, dass $\pi | ab$ und analog für a und b.

2. Jedes Primelement π ist irreduzibel. Denn angenommen $\pi = ab$. Dann muss π entweder a oder b teilen, sagen wir $a = \pi \cdot r$. Dann ist aber $\pi = \pi \cdot r \cdot b$. Also $rb = 1$ und somit b eine Einheit.

3. Die Umkehrung gilt i.A. nicht. In einem PID R aber schon, denn angenommen $p \in R$ is irreduzibel. Wir behaupten, dass dann (p) maximal ist, dann folgt die Behauptung, weil (p) dann prim ist. Dazu sei $(p) \subseteq (a)$, also $a|p$ oder anders gesagt $p = ax$ es folgt, dass entweder a oder x eine Einheit ist, also $(a) = R$ oder $(a) = (p)$.

4. Es folgt, dass in PIDs (wie in $\mathbb{Z}$) gilt, dass ein Primideal $I \neq 0$ bereits maximal ist.

Beispiel 6.5. Im Ring $\mathbb{Z}$ der ganzen Zahlen sind die irreduziblen Elemente genau die Primelemente, also genau die Primzahlen. Im Polynomring $K[x]$ über einem Körper K sind die Irreduziblen Elemente genau die Polynome p die sich nicht als Produkt von Polynomen kleineren Grades schreiben lassen.

Beispiel 6.6. Sie E/K eine Körpererweiterung und $\alpha \in E$. Dann ist $p \in K[x]$ mit $p(\alpha) = 0$ und p normiert genau dann das Minimalpolynom von α, wenn p irreduzibel ist. Denn falls p irreduzibel ist, so stimmt es mit dem Minimalpolynom überein. Falls andersrum p das Minimalpolynom ist, so muss das Ideal (p) maximal und daher prim sein (da der Quotient ein Körper ist), also p irreduzibel.

Im Polynomring (und analog in $\mathbb{Z}$) sieht man, dass sich jedes Element als Produkt von irreduziblen Elementen schreiben lässt, denn man kann induktiv einfacher p entweder als Produkt von Polynomen kleineren Grades schreiben oder es ist bereits irreduzibel. Wir fragen uns nun, wie eindeutig diese Darstellung ist. Dazu formalisieren wir dies zunächst im Begriff des faktoriellen Rings

Definition 6.7. *Ein Integritätsring R heisst faktoriell (engl. UFD unique factorization domain), falls jedes Element $r \neq 0$, $r \notin R^\times$ ein Produkt von Primelementen ist.*

Wir sehen, dass $\mathbb{Z}$ und $K[x]$ faktoriell sind. Jetzt wollen wir daraus Kapital schlagen.

Satz 6.8. *Sei R ein faktorieller Ring. Dann gilt:*

1. *Jedes irreduzible Element ist prim*

2. *Für jedes Element r welches nicht null und keine Einheit ist, ist die die Darstellung $r = \pi_1 \cdot ... \cdot \pi_r$ eindeutig bis auf Permutation der π_i und Multiplikation mit Einheiten (d.h. Ersetzen von π_i durch $\mu\pi_i$ wobei μ eine Einheit ist).*

Proof. Sei $x \in R$ irreduzibel. Schreibe x als Produkt $p_1 \cdot ... \cdot p_r$ von Primelementen. Aufgrund der irrdeduzibilität gilt $r = 1$ und x ist prim.
Angenommen $\pi_1 \cdot ... \cdot \pi_r = \pi'_1 \cdot ... \cdot \pi'_{r'}$. Dann teilt π'_1 das Produkt auf der linken Seite. Daher teilt es einen der Faktoren, obda $\pi'_1 | \pi_1$. Weil π_1 prim ist, insbesondere unzerlegbar, folgt daraus aber, dass $\pi_1 = \mu\pi'_1$ für $\mu \in R^\times$. Wir haben also

$$\pi_2 \cdot ... \cdot \pi_r = \mu \cdot \pi'_2 ... \cdot \pi'_{r'}$$

und fahren induktiv fort. □

Bemerkung 6.9. Ein Integritätsring ist umgekehrt genau dann faktoriell, wenn jede nicht-Einheit, nicht-null Element eine *eindeutige* Darstellung als Produkt von irreduziblen Elementen hat (Übung). Dies wird oft als Definition genommen. Das sieht man auch schon am englischen Namen (unique Factorization domain).

Beispiel 6.10. Der Ring $\mathbb{Z}$ der ganzen Zahlen ist faktoriell. Insbesondere lässt sich jede Zahl eindeutig (bis auf Units und Permutationen) als Produkt von Primzahlen schreiben.

Beispiel 6.11. Der Polynomring $K[x]$ hat eine eindeutige Primfaktorzerlegung. Zum Beispiel für $K = \mathbb{C}$ hat der Polynomring $\mathbb{C}[x]$. Im Letzteren sehen wir, dass die Primelemente genau die Polynom der Form $(x - \alpha)$ für α in $\mathbb{C}$ sind. Die Primfaktorzerlegung ist also einfach die Linearfaktorzerlegung.
Im Ring $\mathbb{Q}[x]$ sind die Primelemente deutlich komplizierter und wir werden im Folgenden Kriterien finden um diese zu bestimmen. Für $p \in \mathbb{Q}[x]$ können wir dann die Zerlegung über $\mathbb{C}$ betrachten und die Zerlegung über $\mathbb{Q}$ muss dann jeweile ein Produkt davon sein.

Explizites Argument für $K[x]$: Prim = irreduzibel. Dann Zerlegung. Dies funktioniert offensichtlich in jedem euklidischen Ring, d.h. euklische Ringe sind faktoriell. Tatsächlich gilt allgmeiner:

Satz 6.12. *Jeder Hauptidealring ist faktoriell.*

Proof. Wir wissen bereits, dass Primelemente und irreduzible Elemente das gleiche sind (Bemerkung 6.4), es reicht also zu zeigen, dass jedes Elemente $r \neq 0$ und r keine Einheit, Produkt von irreduziblen Elementen ist. Falls r irreduzibel ist sind wir fertig. Anderenfalls gilt $r = ab$ wobei weder a noch b Einheiten sind. Falls nun a oder b nicht irreduzibel sind, so fahren wir fort und bekommen induktiv auf diese Weise immer längere Ausdrücke der Form

$$r = r_0 r_1 r_2 ... r_n$$

Wir behaupten, dieser Algorithmus terminiert, d.h. irgendwann sind alle r_i irreduzibel. Falls nicht, so finden wir ein unendlich lange Kette von Teilern

$$..|s_3|s_2|s_1|s_0|r$$

und damit eine unendliche Kette von Idealen

$$(r) \subsetneq (s_0) \subsetneq (s_1) \subsetneq (s_2) \subsetneq ...$$

Die Vereinigung dieser Ideale ist aber ein Ideal (klar). Also ist die Vereinigung gleich (s). Dann gilt aber $s \in (s_n)$ und somit $(s_n) = (s_{n+1}) = ...$ □

Bemerkung 6.13. Die Umkehrung gilt nicht. Wir werden im nächsten Kapitel sehen, dass $\mathbb{Z}[x]$ faktoriell ist. Aber $\mathbb{Z}[x]$ ist kein Hauptidealring wie wir bereits gesehen hatten (Beispiel 5.2).

Lemma 6.14. *Sei R ein Integritätsring. Dann ist $a \in R$ prim genau dann, wenn das konstante Polynom $a \in R[x]$ prim ist.*

Proof. Es gilt

$$R[x]/(a) = (R/a)[x]$$

wie man leicht anhand der universellen Eigenschaften sieht: eine Abbildung $R[x]/a \to S$ in einen Kommutativen ring S ist das gleiche wie eine Abbildung $R[x] \to S$ sodass a auf null geht. Das ist aber das gleiche wie eine Abbildung $R \to S$ die a auf null sendet und ein Element $s \in S$ (das Bild von x). Damit erfülllt aber $R[x]/a$ die universelle Eigenschaft des Polynomringes $(R/a)[x]$. Es gilt also:
a prim in $R[x] \Leftrightarrow R[x]/a$ Integritatätsring $\Leftrightarrow R/a[x]$ integer $\Leftrightarrow$ □

Korollar 6.15. *Falls $R[x]$ faktoriell ist, so ist auch R faktoriell.*

Proof. Sei $x \neq 0$ ein nicht-Einheit in R. Dann schreiben wir es als Produkt von primelementen in $R[X]$. Die muessen alle Grad 0 haben, also haben wir es nach dem vorigen Lemma auch als Produkt in R geschrieben. □

Wir werde naechstesmal die Umkehrung dieser Aussagen zeigen.

7 Das Lemma von Gauß

Heute wollen wir folgenden Satz beweisen:

Satz 7.1 (Gauss)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann ist auch $R[x]$ faktoriell. Ein nicht-konstantes, irreduzibles Polynom $f \in R[x]$ ist auch irreduzibel in $K[x]$.*

Der Satz kann zum Beispiel benutzt werden um zu entscheiden, ob Polynome mit ganzzahligen Koeffizienten irreduzibel über $\mathbb{Q}$ sind. Es ist sehr viel einfacher zu testen ob sie irreduzibel über $\mathbb{Z}$ sind. Zum Beispiel muss man für ein Polynom dritten Grades $a_0X^3 + a_2X^2 + a_1X + 0$ lediglich testen, ob es Nullstellen in $\mathbb{Z}$ besitzt, was man mit sehr einfach testen kann (ausprobieren oder numerisch).

Bemerkung 7.2. Zunächst überlegen wir uns, dass es in faktoriellen Ringen R einen guten Begriff von ggT gibt: für gegebene Elemente a, b können wir beide in Primfaktoren zerlegen und den maximalen gemeinsamen Teiler bilden. Auf die Art und Weise bekommen wir ein Element d sodass jeder weitere gemeinsame Teiler von a, b auch d teilt (dies folgt, da man teilbarkeit einfach in Termen von Primfaktorzerlegungen ausdrücken kann).
Im Gegensatz zu PIDs (siehe Bemerkung 5.4) kann man im Allgmeinen aber den ggT *nicht* also Linearkombination von a und b schreiben. Zum Beispiel gilt in $\mathbb{Z}[x]$, dass die Polynome $2, x$ teilerfremd sind (also den ggT 1 haben)

aber das Polynom 1 kann nicht als Linearkombination dieser beiden Polynome geschrieben werden. Abstrakt betrachtet gilt für die Ideale

$$(a, b) \subseteq (d)$$

aber nicht unbedingt Gleichheit. Tatsächlich ist (d) das minimale Hauptideal, welches das Ideal (a, b) enthält. In beliebigen Ringen muss ein solches minimales Hauptideal (äquivalent ein ggT) nicht existieren. Falls a und b aber teilerfremd sind, so ist 1 stets der ggT im obigen Sinn, selbst wenn R nicht faktoriell ist.
Analog kann man für beliebig viele Elemente in R den ggT definieren (und auch das kgV, was wir aber nicht brauchen werden).

Definition 7.3. *Ein Polynom $f \in R[x]$ für einen Integritätsring R heisst primitiv, falls alle Koeffizienten teilerfremd sind. Falls R faktoriell ist und $f \in R[x]$ so definieren wir den Inhalt von f als das vom* ggT *der Koeffizienten erzeugte Hauptideal in R, d.h.*

$$\mathrm{cont}_R(f) = \mathrm{cont}_R(a_n x^n + ... + a_0) := (\mathrm{ggT}(a_0, ..., a_n)) \subseteq R \ .$$

Das Ideal ist wohldefiniert, da der der ggT bis auf Einheiten eindeutig ist. Wir werden oft auch einen Erzeuger des Ideals (also einen ggT) als Inhalt bezeichnen.

Bemerkung 7.4. Wir können ein Polynom $f \in R[x]$ schrieben als ag mit g primitiv und a ein Repräsentant des Inhalts. Allgmeiner können wir ein Element $f \in K[x]$ schrieben als ag mit $a \in K^\times$ und $g \in R[x]$ primitiv, indem wir zunächst alle Nenner von Elementen in $R[x]$ loswerden und dann durch den Inhalt teilen. Diese Darstellung ist bis auf Einheiten in R eindeutig.
Wir nennen a dann auch den Inhalt des Polynoms f und bezeichnen es mit $\mathrm{cont}_R(f)$. Wichtig ist, sich klarzumachen, dass das von R abhängt. Wir betrachten $\mathrm{cont}_R(f)$ als Element in $K^\times$ welches eindeutig bis auf Einheiten in R ist.
Ein Polynom $f \in K[x]$ is offensichtlich genau dann in $R[x]$, wenn der Inhalt $\mathrm{cont}_R(f)$ in R liegt. [3]

Beispiel 7.5. Wir betrachten $R = \mathbb{Z}$. Es gilt

$$\mathrm{cont}_{\mathbb{Z}}(2x^3 + 6x^2 + 4x) = \pm 2$$

und

$$\mathrm{cont}_{\mathbb{Z}}(x^3 + 3/2x^2 + 2) = \pm 1/2$$

Allgmein ist eine normiertes Polynom über $R[x]$ immer primitiv. Ein normiertes Polynom über $K[x]$ hat als inhalt

Lemma 7.6 (Gauss)**.** *Sei R faktoriell. Dann gilt für $f, g \in K[x]$ die Formel*

$$\mathrm{cont}_R(fg) = \mathrm{cont}_R(f)\,\mathrm{cont}_R(g) \ .$$

[3] In Wahrheit sollte man das als gebrochenes Ideal betracten, das heiss al Teilmenge von K welche abgeschlossen unter Addition und Multiplikation mit R ist.

Proof. Aufgrund der Produktdarstellung reicht es zu zeigen, dass dies für $f, g \in R[x]$ primtiv richtig ist. Es reicht also zu zeigen, dass kein primelement $\pi \in R$ die Koeffizienten von f, g teilt oder äquivalent das konstantes Polynom π teilt nicht fg. Nach Lemma 6.14 ist π aber auch prim im Polynomring. Also falls π das Produkt teilen würde, so müsste es auch einen der Faktoren teilen. □

Beispiel 7.7. In $\mathbb{Z}[x]$ ist das Polynom $f = 6x^7 + 23x^3 + 9x^2 - 12x + 24$ nicht durch $g = 6x^4 + 9x^3 + 3x^2 + 3x + 3$ teilbar, denn der Inhalt von f ist 1 und der von g ist 3.

Korollar 7.8. *Sei R faktoriell. Gegeben ein Polynom $f \in R[x]$. Jede Nullstelle in K kann so geschrieben werden, dass der Nenner ein Teiler des höchsten Koeffizienten und der Zähler ein Teiler des Absolutgliedes ist. Insbesondere falls f normiert ist, liegt jede Nullstelle bereits in R.*

Proof. Sei α/β eine Nullstelle über K mit $\alpha, \beta \in R$ teilerfremd. Dann gilt

$$\mathrm{cont}_R(x - \alpha/\beta) = 1/\beta.$$

über $K[x]$. Wir haben eine Zerlegung

$$f = (x - \alpha/\beta) \cdot g \qquad \text{in} \qquad K[x]$$

sodass $\mathrm{cont}_R(f) = 1/\beta \cdot \mathrm{cont}_R(g)$. Es folgt, dass $\mathrm{cont}_R(g) \in R$ und damit, dass $g \in R[x]$. Der höchste Koeffizient von g ist gleich dem höchsten Koeffizienten von f und dieser wird von $\mathrm{cont}_R(g)$ geteilt werden, was wiederum von β geteilt wird. Schließlich stellen wir fest, dass gilt

$$f(0) = -\alpha/\beta \cdot g(0)$$

sodass α ein Teiler des Absolutgliedes von f ist. □

Beispiel 7.9. $f = 2x^7 + x^3 + x^2 + 3x + 1$ hat keine rationalen Nullstellen, denn die einzig möglichen rationalen Nullstellen wären $\pm 1/2$ und ± 1.
Allgmeiner sagt dieser Satz, dass Nullstellen von Polynomen mit ganzzahligen Koeffizienten entweder ganzzahlig sind, oder irrational. Zum Beispiel sehen wir mit dem Polynom $x^n - m$ sofort, dass wenn m keine m-te Potenz ist, dass alle n-ten Wurzeln aus m irrational sein müssen.

Korollar 7.10. *Sei $f \in R[x]$ mit R faktoriell. Angenommen in $K[x]$ gilt $f = gh$ mit $g, h \in K[x]$ normiert. Dann liegen g und h bereits in $R[x]$.*

Proof. Es gilt $\mathrm{cont}_R(f) = 1/x$ und $\mathrm{cont}_R(g) = 1/y$ für $x, y \in R$, da die Polynome normiert sind. Es muss aber gelten, dass $1/x \cdot 1/y$ eine Einheit in R ist (da das Ideal 1 ist), also müssen x und y bereits selbst in $R^\times$ sein, also die Inhalte der Polynome in R und somit die Polynome in R. □

Korollar 7.11. *Für R ein primitives Polynom $f \in R[x]$ welches irreduzibel über $K[x]$ ist, ist ein Primelement in $R[x]$.*

Proof. Angenommen es gilt $f|gh$. Es folgt über $K[x]$ dass (oBDA) $f|g$, also $g = f \cdot l$ mit $l \in K[x]$. Es folgt sofort aus

$$\text{cont}_R(g) = \text{cont}_R(f) \cdot \text{cont}_R(l) = 1 \cdot \text{cont}_R(l)$$

dass $\text{cont}_R(l) \in R$ und damit $l \in R[x]$ sodas $f|g$ in $R[x]$. □

Satz (Satz 7.1 modifiziert)**.** *Für R faktoriell ist auch $R[x]$ faktoriell und die Primelemente sind genau die Primelemente in R (aufgefasst als konstante Polynome) und die primitiven Primelemente in $K[x]$.*

Proof. Wir wissen nach Satz 7.11 und 6.14 bereits, dass die angegbenen Elemente prim sind. Es reicht also zu zeigen, dass jedes Element sich als Produkt dieser Elemente schreiben lässt. Also sei $f \in R[x]$. Wir schreiben f in $K[x]$ als Produkt

$$f = \lambda\pi_1 \cdot ... \cdot \pi_n$$

mit $\lambda \in K^\times$ and π_i prim. Wir können obda annehmen, dass alle π primitiv sind Es folgt, dass $\lambda \in R$. Zerlegen von λ in R liefert dann die Aussage. □

Wir erinnern daran, dass es uns darum ging Kriterien zu verstehen, mittels derer wir zeigen können, dass Polynome in $\mathbb{Q}[x]$ irreduzibel sind. Falls die Polynome ganzzahlige Koeffizienten haben, folgt aus den vorherigen Überlegungen, dass es reicht zu zeigen, dass sie in $\mathbb{Z}[x]$ nicht zerlegt werden können. Das ist natürlich eine viel einfachere Frage!

Bemerkung 7.12. Was haben wir bisher gesehen? Wenn E/K eine Körpererweiterung ist, so gilt für $\alpha \in E$ dass

$$K(a) \cong K[x]/\min_K(\alpha)$$

wobei $\min_K(\alpha)$ das Minimalpolynom von α über K ist. Dieses ist irreduzibel in $K[x]$. Abstrakt characterisieren kann man es als das eindeutige, irreduzible, normierte Polynom welches α annihiliert. Dann ist

$$[K(\alpha) : K] = \deg \min_K(\alpha \ .$$

Um die Körpererweiterung zu verstehen müssen wir als entscheiden können ob ein Polynom irreduzibel ist. Umgekehrt ist für jedes irreduzible Polynom $p \in K[x]$ der Ring

$$E := K[x]/p$$

eine Köpererweiterung von K (aufgefasst als konstante Polynome). Es gilt $\min_K(x) = p$.
Falls K der Quotientkörper einer faktoriellen Ringes R ist, zum Beispiel $K = \mathbb{Q}$ und $R = \mathbb{Z}$ dann können wir wie folgt vorgehen: gegeben ein Polynom $p \in \mathbb{Q}[x]$ so können wir p schreiben als $\alpha \cdot \tilde{p}$ mit $p \in R[x]$ primitiv und $\alpha = \text{cont}_R(p)$. Wir haben im letzten Kapitel gesehen, dass p genau dann irreduzibel in $K[x]$ ist, wenn $\tilde{p}$ irreduzibel in $R[x]$ ist.

8 Das Eisensteinkriterium

Wir wollen jetzt Kriterien angeben, mit denen man entscheiden kann, ob ein Polynom über $R[x]$ irreduzibel ist. Man kann dies Allgmeiner über beliebigen Integritätsringen studieren (auch wenn wir es auf faktorielle Ringe anwenden werden).

Satz 8.1 (Reduktionskriterium)**.** *Sei R eine Integritätsrings und $f \in R[x]$ primitiv, $I \subseteq R$ ein Primideal und gelte*

1. *das Bild $\overline{f} \in (R/I)[x]$ ist irreduzibel*
2. *der höchste Koeffizient von f liegt nicht in I.*

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

Proof. Sei $f = gh$. Weil f primitiv ist, haben g und h Grad größer gleich 1 (sonst könnte man Koeffizienten rausziehen). Weil der Leitkoeffizient von f in R/I nicht verschwindet, haben die Bilder $\overline{g}$ und $\overline{h}$ ebenfalls Grade ≥ 1 (die Leitkoeffizienten können ebenfalls in R/I nicht verschwinden). Weil R/I integritätsring ist sind somit $\overline{g}$ und $\overline{h}$ keine Einheiten im Widerspruch zur irreduzibilität von f.. □

Beispiel 8.2. Es gilt, dass $x^2 - 2$ irreduzibel in $\mathbb{Z}[x]$ ist, weil es in $\mathbb{F}_3[x]$ irreduzibel ist. Über $\mathbb{F}_3$ hat es nämlich keine Nullstelle wie man leicht durch ausprobieren der Elemente in $\mathbb{F}_3$ sieht. Aber modulo 2 is $x^2 - 2 = x^2 \mod 2$ natürlich reduzibel, also die Umkehrung des Satzes gilt nicht.

Definition 8.3. *Sei R ein Integritätsring. Ein primitves Polynom $f \in R[x]$ der Form*

$$f(x) = a_n x^n + ... + a_0$$

heisst Eisensteinpolynom *falls es ein Primelement $\pi \in R$ gibt, sodass gilt*

1. *π teilt nicht den Leitkoeffizienten a_n*
2. *π teilt alle anderen Koeffizienten $a_{n-1}, ..., a_0$.*
3. *π^2 teilt nicht a_0.*

Wir sagen auch, dass f ein Eisensteinpolynom bezüglich π ist.

Satz 8.4 (Eisensteinkriterium)**.** *Jedes Eisensteinpolynom $f \in R[x]$ ist irreduzibel. Insbesondere falls R faktoriell ist, so ist es auch irreduzibel in $K[x]$, wobei K der Quotientenring von R ist.*

Proof. Angenommen wir haben eine nicht-triviale Zerlegung $f = gh$ in $R[x]$. Weil f primitiv ist, haben g und h grad ≥ 1. Aus den ersten beiden Bedinungen folgt, dass für die induzierte Zerlegung in R/π

$$\overline{a_n} x^n = \overline{f} = \overline{g}\overline{h}$$

von der Form $\overline{g} = \lambda x^k$ und $\overline{h} = \mu x^l$ mit $k + l = n$ und $k, l \geq 1$ ist. Es folgt, dass in R sowohl $\overline{g}(0) = 0$ also auch $\overline{h}(0) = 0$ gilt. Also teilt π sowohl das Absolutglied von g, wie auch das von h. Dies ist im Widerspruch dazu, dass π^2 nicht a_0 teilt. □

Wir werden das Eisensteinkriterium vor allem auf normierte Polynome anwenden, da Minimalpolynome normiert sind. Normierte Polynome sind immer primitiv und auch die erste Bedingung der Definition ist automatisch erfüllt.

Beispiel 8.5. Das Polynom $x^4 + 4x + 2$ ist irreduzibel über $\mathbb{Z}[x]$ weil es ein Eisensteinpolynom ist bezüglich 2 ist.

Beispiel 8.6. Betrachte das Polynom $x^n - a$ über $\mathbb{Z}[x]$. Falls eine Primzahl p existiert die a teilt, aber sodass p^2 nicht a teilt (äquivalent: a hat mindestens einen einen einfachen Primfaktor), dann ist das Polynom ein Eisensteinpolynom. Es folgt, dass es Irreduzibel über $\mathbb{Q}[x]$ ist. Daher ist dies das Minimalpolynom für (jede) n-te Wurzel von a in $\mathbb{C}$, anders gesagt ist die Erweiterung

$$\mathbb{Q}(\sqrt[n]{a}) \subseteq \mathbb{C}$$

für jede Wahl von n-ter Wurzel von a isomorph zu $\mathbb{Q}[x]/(x^n - a)$ und vom Grad n. (Typischerweise meint man mit $\sqrt[n]{a}$ die reelle oder rein imaginäre Wurzel).

Bemerkung 8.7. Reduktionskriterium und Eisensteinkriterium sind nicht hinreichende Kriterien, aber es gibt irreduzible Polynome in $\mathbb{Z}[x]$ wo weder das eine noch das andere sich anwenden lässt.

Korollar 8.8. *Für eine Primzahl p ist das* zyklotomische Polynom

$$\Phi_p(x) = x^{p-1} + x^{p-2} + ... + 1 = \frac{x^p - 1}{x - 1}$$

irreduzibel in $\mathbb{Z}[x]$ und damit auch in $\mathbb{Q}[x]$. Es ist also das Minimalpolynom von $\zeta_p = \exp(2\pi i/p) \in \mathbb{C}$ über $\mathbb{Q}$ und daher gilt

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 \ .$$

Proof. Das Polynom selbst ist kein Eisensteinpolynom. Wir betrachten den Ringisomorphismus

$$f : \mathbb{Z}[x] \xrightarrow{\simeq} \mathbb{Z}[y] \qquad x \mapsto y + 1 \ .$$

Dies ist ein Isomorphismus, denn es gibt den Inversen $y \mapsto x - 1$. Um zu zeigen, dass Φ_p irreduzibel ist, reicht es also zu zeigen, dass das Bild

$$f(\Phi_p) = \Phi_p(y + 1) = \frac{(y + 1)^p - 1}{y} = y^{p-1} + py^{p-2} + \binom{p}{2} y^{p-3} + ... + p$$

Dieses Polynom ist ein Eisensteinpolynom, da alle Binomialkoeffizienten

$$\binom{p}{k} = \frac{p!}{k!(p - k)!}$$

für $1 \leq k \leq p - 1$ durch p-teilbar sind (der Zähler ist durch p teilbar, aber der Nenner nicht). □

Korollar 8.9. *Sei p eine Primzahl. Ist $p - 1$ keine Potenz von 2, so ist die Konstruktion des regulären p–Ecks mit Zirkel und Lineal nicht möglich.*

Proof. Folgt aus Korollar 2.14 und Korollar 8.8. □

Bemerkung 8.10. Eine Primzahl p für die $p-1$ eine 2-er Potenz ist, ist eine sogenannte *Fermat Primzahl*. man kann sich leicht überlegen, dass diese schon von der Form $p = 2^{2^k} + 1$ sein. Die ersten 5 Zahlen (d.h. k=0,..,4) sind tatsächlich Primzahlen, nämlich $3, 5, 17, 257, 65537$. Die nächste Fermatzahl $2^{2^5} + 1$ ist schon sehr groß, allerdings keine Primzahl (wie von Euler gezeigt). Damit widerlegte er Fermat's Vermutung, dass alle diese Zahlen Prim sind. Tatsächlich kennt man keine weiteren Fermat Primzahlen und es gibt die Vermutung, dass es nur diese 5 gibt. Insbesondere sehen wir, dass die Konstruierbarkeit eine signifkante Einschränkung and das p-Eck ist.

Unser Ziel wird es im Folgenden sein auch die Minimalpolynome der Einheitswurzeln ζ_n und damit den Grad der Körpererweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ zu bestimmen. Wir stellen dazu fest, dass das Minimalpolynom von ζ_n das Polynom $z^n - 1$ teilen muss, da letzteres ζ_n annihiliert. Aus Korollary 7.11 folgt dann, dass $\min_{\mathbb{Q}}(\zeta_n)$ bereits ganzzahlig sein muss (da es normiert ist).
Wir haben ebenso die Minomalpolynom der anderen n-ten Einheitswurzeln

$$\min_{\mathbb{Q}}(\zeta_n^k) \in \mathbb{Q}[x] \qquad \text{für } k = 1, 2, ...$$

Diese teilen ebenfalls $z^n - 1$, sind damit ebenfalls ganzzahlig und aus Gradgründen bekommen wir, dass $z^n - 1$ das Produkt gewisser solcher Polynom ist. Anschaulich gesprochen müssen wir also versuchen

$$z^n - 1 = \prod_{k=1}^{n}(z - \zeta_n^k)$$

in $\mathbb{Z}[x]$ zu zerlegen, oder äquivalent die Faktoren so zu kombinieren, dass die Polynome ganzzahlig werden. Dies liefert dann die Minimalpolynome von den Einheitswurzeln (wobei gewisse Polynome mehrfach vorkommen). In der nächsten Vorlesung werden wir dies genauer analysieren und am Ende die genauen Minimalpolynome und Grade von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ bestimmen.

9 Gruppen und Einheitswurzeln

Definition 9.1. *Für eine beliebige natürliche Zahl n sei*

$$\mu_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\}$$

die Gruppe der n-ten Einheitswurzeln. Dies ist eine Gruppe unter Multiplikation (da unter Produkten und Inversenbildung abgeschlossen). Es sei

$$\mu_n'(\mathbb{C}) = \{z \in \mu_n(\mathbb{C}) \mid z^k \neq 1 \forall k < n\}$$

Die Elemente werden primitive *Einheitswurzeln genannt.*

Beispiel 9.2. Für $n = 1$ gilt $\mu_1(\mathbb{C}) = \{1\}$ und für $n = 2$ gilt $\mu_2(\mathbb{C}) = \{1, -1\}$ und -1 ist primitiv. Bild für ζ_6 malen.
Es gilt offensichtlich für $\zeta_n = \exp(2\pi i/n) \in \mu_n(\mathbb{C})$, dass

$$\mu_n(\mathbb{C}) = \{\zeta_n, \zeta_n^2, ..., \zeta_n^{n-1}\} \ .$$

Eine andere Art dies auszudrücken ist, dass wir einen Gruppenisomorphismus haben

$$(\mathbb{Z}/n, +) \to \mu_n(\mathbb{C}) \qquad k \mapsto \zeta_n^k \ .$$

Um die primitive Einheitswurzeln besser zu verstehen führen wir ein paar elementare Begriffe der Gruppentheorie ein.

Definition 9.3. *Sei $H \subseteq G$ eine Untergruppe. Wir definieren eine Äquivalenzrelation auf G durch*

$$g \sim g' :\Leftrightarrow g^{-1}g' \in H$$

und schreiben die Menge der Äquivalenzklassen als G/H. Die Äquivalenzklasse von $g \in G$ wird geschrieben als $[g] \in G/H$.

Es ist offensichtlich, dass dies eine Äquivalenzrelation ist (nachrechnen!).

Beispiel 9.4.

1. Als Teilmenge von G haben wir $[g] = gH \subseteq G$.
2. Für die (additive) Gruppe $\mathbb{Z}$ mit der Untergruppe $n\mathbb{Z}$ ist $\mathbb{Z}/n\mathbb{Z}$ genau die Menge der Restklassen wie vorher schon betrachtet.
3. Für die symmetrische Gruppe Σ_3 der Permutation der Menge $\{1, 2, 3\}$ mit der Untergruppe $\Sigma_2 \subseteq \Sigma_3$ betrachtet als Permutationen von $\{1, 2\}$, d.h die Elemente in Σ_3 festlassen. Diese Untergruppe hat die zwei Elemente id und (12). Dann sind die Äquivalenzklassen:

$$\{\mathrm{id}, (12)\} \qquad \{(13), (123)\} \qquad \{(23), (132)\}$$

Satz 9.5 (Lagrange)**.** *Sei G eine endliche Gruppe und $H \subseteq G$. Dann gilt*

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

Insbesondere teilt die Ordnung jeder Untergruppe die Gruppenordnung.

Proof. Jeder Äquivalenzklasse ist von der Form gH, also in Bijektion zu H durch die Abbildung

$$H \xrightarrow{\simeq} gH \qquad h \mapsto gh$$

Wir haben eine disjunkte Zerlegung

$$G = \coprod gH$$

Daraus folgt die Formel für die Kardinalität. □

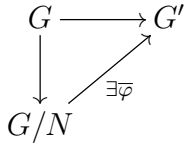
Es folgt zum Beispiel, dass Gruppen von Primzahlordnung nur die trivialen Untergruppen $\{1\}$ und G haben können. Allgmeiner kann man damit die Ordnung von Untergruppen schnell eingrenzen.

Definition 9.6. *Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ heisst Normalteiler, falls für jedes Element $g \in G$ und $n \in N$ gilt $gng^{-1} \in N$.*

Beispiel 9.7.
1. Für einen Gruppenhomomorphismus $\varphi : G \to H$ ist der Kern ein Normalteiler. Denn $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(G)^{-1} = 1$.
2. Allgmeiner ist für einen Normalteiler $N \subseteq H$ auch das Urbild $\varphi^{-1}(N)$ ein Normalteiler, denn für $n \in \varphi^{-1}(N)$ (äquivalent $\varphi(n) \in N$) gilt
$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} \in N.$$
3. Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.
4. Das Zentrum $Z(G) = \{z \in G \mid \forall h \in G : zh = hz\} \subseteq G$ ist ein Normalteiler, denn für $z \in Z(g)$ gilt $gzg^{-1} = z \in Z(G)$.

Satz 9.8 (Quotientengruppe)**.** *1. Falls N ein Normalteiler ist, so hat G/N die eindeutige Struktur einer Gruppe sodass die Projektion $\pi : G \to G/N$ ein Gruppenhomomorphismus ist.*

2. G/H erfüllt dann die universelle Eigenschaft, dass für jeden Gruppenhomomorphimus $\varphi : G \to G'$ mit $N \subseteq \ker(\varphi)$ ein eindeutiger Homomorphismus



3. Es gilt, dass $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$ und $\ker(\overline{\varphi}) = \ker(\varphi)/N$. Insbesondere haben wir $\mathrm{Im}(\varphi) = G/\ker(\varphi)$.

Isomorphiesatz

Proof. Für den ersten Teil des Beweises stellen wir fest, dass die Abbildung $\pi : G \to G/N$ das Element $g \in G$ auf die Äquivalenzklasse $[g] = gN \subseteq G$ schickt. Damit dies ein Gruppenhomomorphismus wird müssen wir als haben, dass
$$[g][g'] = [gg']$$
Wir müssen also zeigen, dass diese Multiplikation wohldefiniert ist (analog zum Fall von Ringen und Idealen, den wir ausgelassen haben). Sei also $g \sim h$. Wir zeigen, dass $gg' \sim hg'$. Die Wohldefiniertheit in der anderen Variable geht analog. Wir haben, dass $g^{-1}h \in N$. Also folgt, dass
$$(gg')^{-1}hg' = (g')^{-1}g^{-1}hg' \in H$$
da H ein Normalteiler ist. Dies zeigt die Wohldefiniertheit. Der Rest geht komplett analog zum Fall von Ringen und Idealen (Satz 4.7)). □

Beispiel 9.9. Für Vektorräume $U \subseteq V$ hat der Quotientenraum V/U also unterliegende abelsche Gruppe die Quotientengruppe. Das gleiche gilt für den Quotienten eines Ringes nach einem Ideal.

Definition 9.10. *1. Sei $g \in G$. Die Ordnung* $\mathrm{ord}(g)$ *von g ist die kleinste positive natürliche Zahl mit $g^n = 1$ falls ein solches existiert, sonst ist die Ordnung unendlich.*

2. Für eine Teilmenge $S \subseteq G$ einer Gruppe definieren wir die von S erzeugte Untergruppe $\langle S \rangle$ als den Durschnitt aller Untergruppen die S enthalten. Für ein Element $g \in G$ ist

$$\langle g \rangle = \{1, g, g^2, ..., g^{\mathrm{ord}(g)-1}\}$$

3. Eine Gruppe heisst zyklisch, falls sie von einem Element erzeugt wird, d.h. es gibt ein Element $g \in G$ sodass $\langle g \rangle = G = \{1, g, g^2, g^3, ..., \}$. Das Element g heisst dann Erzeuger.

Bemerkung 9.11. 1. Jede Gruppe von Primzahlordnung ist zyklisch, denn für jedes Element $g \in G$ ist die erzeugte Untergruppe $\langle g \rangle = G$. Sie wird also auch von jedem Element erzeugt.

2. Die Gruppe $(\mathbb{Z}/n, +)$ ist zyklisch, zum Beispiel erzeugt von dem Element 1. Aber nicht jedes Element erzeugt die Gruppe. Zum Beispiel ist in $\mathbb{Z}/4$ das Element 2 von Ordnung 2.

3. Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}/n$ wobei $n = 0$ falls $|G| = \infty$ und $n = |G|$ sonst. Ein Isomorphismus ist gegeben durch

$$\mathbb{Z}/n \to G \qquad n \mapsto g^n$$

Diese Abbildung ist offensichtlich wohldefiniert, injektiv und surjektiv (per Definition). EinE

4. Die primitiven Einheitsqwurzeln sind genau die Erzeuger von $\mu_n(\mathbb{C})$.

5. Untergruppen zyklischer Gruppen sind zyklisch. Um dies zu sehen stellen wir zunächst fest, dass Untegruppen von $\mathbb{Z}$ genau die Ideale sind, also von der Form $n\mathbb{Z}$ und daher isomorph zu $\mathbb{Z}$ selbst. Für eine beliebige zyklische Gruppe sind Untergruppen $U \subseteq G$ unter dem Iso aus (3) (welcher von der Wahl eines Elementes $g \in G$ abhängt) genau die Untergruppen von $\mathbb{Z}$ die $n\mathbb{Z}$ enthalten. Also selbst zyklisch.

Korollar 9.12. *(Kleiner Satz von Fermat) Für endliche Gruppen teilt die Ordnung jedes Elementes die Gruppenordnung (nach Lagrange). Es folgt, dass*

$$g^{|G|} = 1 \ .$$

Korollar 9.13. *Für $k \in \mathbb{Z}$ sind äquivalent:*

1. $\mathrm{ggT}(k, n) = 1$

2. $[k]$ ist eine Einheit im Ring $\mathbb{Z}/n$.

3. $[k]$ ist ein Erzeuger der Gruppe $\mathbb{Z}/n$

Proof. 1) $\Rightarrow$ 2): Wähle nach dem Lemma von Bézout $a, b \in \mathbb{Z}$ sodass $ak+bn = 1$. Dann ist $[a]$ das Inverse von $[k]$ in $\mathbb{Z}/n$. Umgekehrt folgt (2) $\Rightarrow$ (1) da wir für eine Einheit k ein Element a haben sodass $ak = 1 + bn$.

2) $\Rightarrow$ 3) k ist genau dann eine Einheit wenn die Multiplikation mit $k : \mathbb{Z}/n \to \mathbb{Z}/n$ injektiv ist (da injektiv und bijektiv äquivalent sind). Daher sind die Vielfachen $k, 2k, 3k, 4k, ..., (n-1)k, nk$ alle verschieden und daher ist die von k erzeugte Untergruppe alles. Umgekehrt genauso. □

Es folgt insbesondere, dass

$$\mu'_n(\mathbb{C}) = \{\exp(2\pi ik/n) \mid 0 \leq k < n, \text{ggT}(k, n) = 1\} \cong (\mathbb{Z}/n)^\times.$$

Der Ordnung dieser Gruppe geben wir nun einen Namen. Die Gruppenstruktur auf $\mu'_n(\mathbb{C})$ induziert von diesem Isomorphismus ist *nicht* von der Multiplikativen Struktur von $\mathbb{C}$ induziert, sie ist gewissermaßen nicht-kanonisch, da man eine Einheitswurzel auswählen muss um den Isomorphismus zu bekommen.

Definition 9.14. *Wir definieren die Euler'sche ϕ-Funktion als*

$$\phi(n) := |(\mathbb{Z}/n)^\times|$$

Bemerkung 9.15.

1. Es gilt für p prim, dass $\varphi(p) = p - 1$.
2. Für m teilerfremd zu n gilt Es gilt $m^{\varphi(n)} = 1 \mod n$ (Satz von Euler) nach dem Satz von Lagrange angewendet auf die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$.
3. Für Primzahlen p und $m \in \mathbb{Z}$ folgt
$$m^p = m \mod p$$
4. Für eine Primzahlpotenz gilt $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
5. Für teilerfremde Zahlen m, n gilt
$$(\mathbb{Z}/mn)^\times = (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$$
Also $\varphi(mn) = \varphi(m) \times \varphi(n)$.
6. Mit 4 und 5 kombiniert bekommt man eine Allgmeiner Formel für $\varphi(n)$ in Termen der Primfaktorzerlegung von n.

Wir schließen das Kapiter der Feststellung, dass wir eine Zerlegung als Mengen haben

$$\mu_n(\mathbb{C}) = \coprod_{k|n} \mu'_k(\mathbb{C}) \ .$$

Diese Zerlegung werden wir im kommenden Kapitel benutzen um die Minimalpolynome der Einheitswurzeln ζ_n zu bestimmen (die sogenannten zyklotomischen Polynome).

10 Zyklotomische Polynome

In diesem Kapitel wollen wir schließlich die Minimalpolynome der Elemenrte ζ_n für jedes $n > 0$ bestimmen und damit die Grade der Körpererweiterungen $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Wir haben dies bereits für $n = p$ prim bestimmt und festgestellt, dass das Minimalpolynom von ζ_n ein Teiler von $x^n - 1$ sein muss und damit ein Produkt von Linearfaktoren der Form $(x - \zeta_n^k)$.

Wir erinnern daran, dass wir mit $\mu_n(\mathbb{C})$ die n-ten Einheitswurzeln bezeichnen und mit $\mu'_n(\mathbb{C}) \subseteq \mu_n(\mathbb{C})$ die primitiven n-ten Einheitswurzeln. Für $k|n$ haben wir eine Inklusion $\mu_k(\mathbb{C}) \subseteq \mu_n(\mathbb{C})$ und damit auch eine Inklusion $\mu'_k(\mathbb{C}) \to \mu_n(\mathbb{C})$. Damit haben wir

$$\mu_n(\mathbb{C}) = \coprod_{k|n} \mu'_k(\mathbb{C}) \ .$$

Definition 10.1. *Wir definieren das n-te zyklotmische Polynom (aka Kreisteilungspolynom) als*

$$\Phi_n(x) = \prod_{z \in \mu'_n(\mathbb{C})} (x - z) \in \mathbb{C}[x] \ .$$

Der Grad des zykltomischen Polynomes $\Phi_n(x)$ ist $\phi(n)$.

Beispiel 10.2. Wir listen die ersten paar Polynome auf:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= (x + 1) \\
\Phi_3(x) &= (x - \zeta_3)(x - \zeta_3^2) = x^2 + x + 1 \\
\Phi_4(x) &= (x - i)(x + i) = x^2 + 1 \\
\Phi_5(x) &= \frac{x^n - 1}{x - 1} = x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= (x - \zeta_6)(x - \zeta_6^5) = x^2 - x + 1
\end{aligned}$$

Für Primzahlen gilt $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^p + x^{p-1} + ... + 1$ sodass die Definition mit der in Korollar 8.8 gegebenen übereinstimmt und das Polynom das Minimalpol von ζ_p ist (und auch allen anderen primitiven p-ten Einheitswurzeln). Wie werden bald sehen, dass alle zyklotomischen Polynome irreduzibel sind und damit die Minimalpolynome von allen primitiven Einheitswurzeln sind.

Satz 10.3. *Die zykltomischen Polynome sind alle ganzzahlig, d.h. $\Phi_p(x) \in \mathbb{Z}[x]$ und es gilt*

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \ .$$

Proof. Die Gleichung folgt sofort aus der Zerlegung der Einheitswurzeln

$$\mu_n(\mathbb{C}) = \coprod_{k|n} \mu'_k(\mathbb{C}) \ .$$

Wir können dann induktiv $\Phi_n(x)$ durch Polynomdivision berechnen als

$$\Phi_n(x) = (x^n - 1) / \prod_{d|n\, d<n} \Phi_d(x)$$

Falls wir bereits wissen, dass die $\Phi_d(x)$ ganzzahlig sind, so folgt, dass $\Phi_n(x) \in \mathbb{Q}[x]$ und dann mit dem Gausslemma (alle Polynome sind normiert) dass es bereits ganzzalig ist.

□

Bemerkung 10.4. Mit der Formel kann man rekursiv sehr schnell die $\Phi_n(x)$ bestimmen. Wenn man dies tut stellt man zunächst fest, dass alle auftretenden Koeffizienten ± 1 und 0 sind. Man kann sich fragen ob dies stets der Fall ist - die Antwort lautet 'nein'. Das erste Gegenbeispiel ist

$$\begin{aligned}\Phi_{105}(x) = & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - x^7 - x^6 - x^5 + x^2 + x + 1 \ .\end{aligned}$$

Tatsächlich werden die Koeffizienten beliebig groß.

Satz 10.5. *Das n-te zyklotomische Polynom $\Phi_n(x)$ ist irreduzibel. Es ist also das Minimalpolynom aller primitiver n-ter Einheitswurzel und es gilt*

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Wir werden den Satz am Ende des Kapitels mittels einiger Hilfsaussagen beweisen, zunächst möchten wir ein paar Konsequenzen ziehen.

Korollar 10.6. *Für jede primitive Einheitswurzel $z \in \mathbb{C}$ gibt es einen eindeutigen Körperautomorphismus $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ welcher ζ_n auf z schickt. Umgekehrt ist jeder Körperendomorphismus von dieser Form (insbesondere ein Automorphismus).*

Proof. Es gilt $\mathbb{Q}(\zeta_n) = \mathbb{Q}[x]/\Phi_n(x)$. Also ist ein Körperhomomorphismus

$$\mathbb{Q}(\zeta_n) \to K$$

in jedem Körper K über $\mathbb{Q}$ dadurch bestimmt, wohin er ζ_n schickt, und man kann ζ_n auf jede Nullstelle von $\Phi_n(x)$ in K schicken. Diese Nullstellen für $K = \mathbb{Q}(\zeta_n)$ sind genau die primitiven Einheitswurzeln. □

Es gilt also isbesondere, dass die Gruppe der Körperautomorphismen durch

$$\mathrm{Aut}(\mathbb{Q}(\zeta_p)) \cong (\mathbb{Z}/n)^\times$$

isomorph ist zur Gruppe der Einheiten in $\mathbb{Z}/n$.

Korollar 10.7. *Das regelmäßige n-Eck ist höchstens dann mit Zirkel und Lineal konstruierbar, wenn n von der Form $n = 2^k \cdot p_1 \cdot \ldots \cdot p_k$ für paarweise verschiedene Fermat'sche Primzahlen gilt.*

Wir erinnern daran, dass Fermat'sche Primzahlen diejenigen Primzahlen der Form $2^{2^m}+1$ sind. Vermutungsweise gibt es nur fünf Fermat'sche Primzahlen: $3, 5, 17, 257, 65537$. Wir werden später mithilfe der Galoistheorie sehen, dass diese Bedinung auch hinreichend ist (wir also $\mathbb{Q}(\zeta_n)$ in dem Fall als iterierte Erweiterung zweiten Grades schreiben können).

Proof. Nach Korollar 2.14 und Satz 10.5 ist eine notwendige Bedingung für die Konstruierbarkeit, dass $\varphi(n)$ eine Zweierpotenz ist. Falls gilt $p^k|n$ dann folgt nach Bemerkung 9.15, dass $(p-1)p^{k-1}$ ein Teiler von $\varphi(n)$ ist. Also muss damit $\varphi(n)$ eine Zweierpotenz ist entweder $p=2$ sein oder $k=1$ und $p-1$ eine Zweierpotenz, also p eine Fermat Primzahl.[4] □

Nun kommen wir zum Beweis von Satz 10.5, also zur Irreduzibilität von Φ_n. Dazu benötigen wir eine weitere Aussagen.

Proposition 10.8. *Sei R ein kommutativer Ring mit $p=0$ für eine Primzahl p. Dann ist die Abbildung*

$$\varphi_p : R \to R \qquad r \mapsto r^p$$

ein Ringhomomorphismus, gennant der Frobenius-Homomorphismus.

Proof. Übungen. □

Beispiel 10.9.

1. Für $R = \mathbb{F}_p = \mathbb{Z}/p$ gilt $\varphi_p = \mathrm{id}$, denn es gilt für jedes $x \in \mathbb{F}_p$ nach dem Satz von Euler, dass $x^p = x$.
2. Für $f \in \mathbb{F}_p[x]$ gilt $f(x^p) = f(x)^p$. Dies folgt daraus, dass

$$(f)^p = \varphi_p(f) = \varphi_p(\sum a_i x^i) = \sum \varphi_p(a_i) x^{pi} = f(x^p)$$

Sie kennen die Ableitung aus der Analysis. Wir können diese tatsächlich (ohne irgendwelche Konvergenzüberlegungen oder Grenzwerte) auf den Polynomring $K[x]$ fortsetzen:

$$(-)' : K[x] \to K[x] \qquad f = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=1}^{n} i a_i x^{i-1} = f'$$

Hier ist K ein Körper, aber tatsächlich funktioniert das alles auch über kommutativen Ringen.

Lemma 10.10. *Es gilt $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$.*

Proof. Nachrechnen. □

Proposition 10.11. *Angenommen für $f \in K[x]$ gilt dass f und f' teilerfremd sind. Dann hat f keine mehrfachen Faktoren und insbesondere keine doppelten Nullstellen.*

[4] Wir erinnern daran, dass eine Primzahl der Form $2^k - 1$ automatisch von der Form $2^{2^m}+1$ ist.

Proof. Falls $f = g^2 h$ dann gilt

$$f' = 2gg'h + g^2 h' = g(2g'h + gh')$$

Also sind f und f' nicht teilerfremd. □

Beispiel 10.12. Wir betrachten das Polynom $x^n - 1$. Dann ist die Ableitung gegeben durch nx^{n-1}. Falls in K gilt $n \neq 0$ so hat nx^{n-1} als Primfaktor nur x. Aber $x^n - 1$ wird nicht von x geteilt. Also sind die Polynome teilerfremd und damit folgt, dass $x^n - 1$ keine doppelten Faktoren in $K[x]$ hat.
Falls $n = 0$ in K gilt, so gilt dieser Schluss nicht, zum Beispiel gilt in $\mathbb{F}_2[x]$ dass $x^2 - 1 = (x-1)(x+1) = (x-1)^2$.

Lemma 10.13. *Sei z eine n-te Einheitswurzel in $\mathbb{C}$ und p eine Primzahl die n nicht teilt. Dann haben z und z^p das gleiche Minimalpolynom über $\mathbb{Q}$.*

Proof. Sei $f = \min_{\mathbb{Q}}(z)$. Wir müssen zeigen, dass $f(z^p) = 0$. Angenommen das ist nicht der Fall. Es gilt

$$x^n - 1 = fg$$

mit $g \in \mathbb{Z}[x]$ nach Gauss. Weil z^p eine n-te Einheitswurzel ist und $f(z^p) \neq 0$ muss also gelten, dass $g(z^p) = 0$. Das Polynom $g(x^p)$ annihiliert also z und muss daher vom Minimalpolynom f geteilt werden:

$$f(x)h(x) = g(x^p) \ .$$

Es folgt wieder aus dem Gauss Lemma, dass $h \in \mathbb{Z}[x]$. Jetzt betrachten wir die Bilder der Polynome unter der Reduktionsabbildung $\mathbb{Z}[x] \to \mathbb{F}_p[x]$. Dort gilt

$$\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$$

Also teilt jeder Primfaktor von $\overline{f}$ das Polynom $\overline{g}$ und diese sind damit nicht teilerfremd. Das kann aber nicht sein, dann dann hatte

$$x^n - 1 = \overline{f}\overline{g}$$

einen doppelten Primfaktor, im Widerspruch zu Beispiel 10.9, da n nicht von p geteilt wird und daher $[n] \neq 0$ in $\mathbb{F}_p$. □

Jetzt können wir schließlich Satz 10.5 beweisen.

Beweis von Satz 10.5. Jede primitive n-te Einheitswurzel ist von der Form ζ_n^k für k teilerfremd zu n. Also ist k von der Form $p_1 \cdots p_s$ mit p_i Primzahlen die n nicht teilen. Wir wenden nun Lemma 10.13 iterativ an um zu sehen, dass

$$\zeta_n, \zeta_n^{p_1}, \zeta_n^{p_1 p_2}, ..., \zeta_n^k$$

alle das gleiche Minimalpolynom haben. Insbesondere haben alle primitiven Einheitswurzeln das gleiche Minimalpolynom und da diese alle verschieden sind folgt, dass das Minimalpolynom von $\Phi_n(x)$ geteilt wird und daher damit übereinstimmt. □

Zusammenfassung bisher

Was haben wir bisher in der Vorlesung gemacht. Am wichtigsten ist bisher die Körpertheorie:

1. Definition eines Körpers

   Beispiel. $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}(\zeta_n)$, $\mathbb{Q}(\sqrt{b})$, $\mathbb{F}_p$, $\mathbb{F}_4$, $K(x)$,...

2. Körperhomomorphismus $f : K \to E$. Sind immer injektiv, E wird dadurch ein K-Vektorraum. Wir sagen dann auch, dass E eine Körpererweiterung von K ist und schreiben E/K.

   Beispiel. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, $\mathbb{F}_4/\mathbb{F}_2$,
   $\mathbb{K}[x]/p$ ist eine Körperwereiterung von K für $p \in K[x]$ irreduzibel
   Für $\mathrm{char}(K) = p$ (i.e. $p = 0$ in K) existiert der Frobenius $\Phi_p : K \to K$.

3. Grad $[E/K] := \dim_K(E)$.

   Beispiel. Es gilt $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ für p prim.
   $[\mathbb{K}[x]/p : K] = \deg(p)$
   $[\mathbb{C}/\mathbb{Q}] = \infty$

4. Für Turm $K \to F \to E$ gilt die Gradformel

   $$[E/K] = [E/F] \cdot [F/K]$$

   Insbesondere teilt der Grad von Zwischenkörpern den Grad von E/K.

   Beispiel. Nicht-triviale Zwischenkörper von $\mathbb{Q}(\zeta_6)$ können nur Grad 2 und 3 haben (gibt es die auch?).

5. E/K Körpererweiterung, $S \subseteq E$, dann existiert $K \subseteq K(S) \subseteq E$ kleinste Körpererweiterung die S enthält. Wir sagen: wir adjungieren S zu K.

6. Insbesondere interessieren wir uns für Körpererweiterungen die durch adjungieren von Quadratwurzeln entstehen, d.h $K(a)$ mit $b = a^2 \in K$. Wir schreiben dies auch als $K(\sqrt{b})$.

   Bemerkung. A priori ist $K(\sqrt{b})$ für $b \in K$ also dann definiert für eine Inklusion $K \subseteq E$ in der eine Wurzel von b existiert. Wir können dies für ein Element $b \in K$ welches keine Wurzel in K hat auch definieren als

   $$K\left(\sqrt{b}\right) := K[x]/(x^2 - b)$$

   Dies ist ein Köper, da $x^2 - b$ irreduzibel in $K[x]$ ist (sonst hätte es eine Nullstelle).

   Quadratische Erweiterungen haben Grad 2. Die Umkehrung gilt in Körpern der Charakteristik $\neq 2$ (sonst Gegenbeispiel $\mathbb{F}_4$).

7. Wir betrachten die konstruierbaren Element in $\mathbb{C}$, d.h. die Elemente die mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar sind. Diese Elemente bilden einen Unterkörper:

   Satz. *Ein Element $z \in \mathbb{C}$ ist kontruierbar, genau dann, wenn es in einer Körpererweiterung liegt die durch sukzessives adjungieren von Quadratwurzeln enststeht. Insbesondere gilt dann $[\mathbb{Q}(z) : \mathbb{Q}] = 2^k$.*

   Beispiel. π ist nicht konstuierbar (da transzendent)
   $\sqrt[3]{2}$ ist nicht konstruierbar, da $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
   ζ_p ist nicht konstuierbar (p prim), falls p kleine Fermatprimzahl, d.h. nicht von der Form $2^{2^k} + 1$.

8. Definition Algebraische und Transzendente Elemente und algebraischen Körpererweiterung.

   Ein Element α ist genau dann algebraisch, wenn $[K(\alpha) : K]$ endlich ist. Äquivalent, wenn $K[\alpha] = K(\alpha)$. Summe und Produkt algebraischer Elemente sind algebraisch. Die Menge der algebraischen Elemente $\overline{K}$ in E bilden einen Unterkörper. Die Komposition von algebraischen Körperwerweiterungen ist algebraisch.

   Beispiel. $\mathbb{C}/\mathbb{R}$ ist algebraisch, $\mathbb{C}/\mathbb{Q}$ nicht, $\mathbb{K}[x]/p$ ist algebraisch über K, $K(x)$ ist transzendent über K. $\overline{\mathbb{Q}}/\mathbb{Q}$ ist algebraisch.

9. Minimalpolynom $\min_K(\alpha) \in K[x]$ eines algebraischen Elementes $\alpha \in K$: mininales normiertes Polynom welches annihiliert, äquivalent: Erzeuger der Annihilatorideals, äquivalent: Irreduzibles Poiynom welches α annihiliert.

   Das Minimalpolynom ist irreduzibel und Es gilt $K(\alpha) = K[x]/\min_K(\alpha)$ und daher $[K(\alpha) : K] = \deg \min_K(\alpha)$.

   Beispiel. In $K[x]/p$ hat x Minimalpolynom p.
   Das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + 1$
   Das Minimalpolynom von $i \in \mathbb{C}$ über $\mathbb{R}$ ist $x^2 + 1$.
   Das Minimalpolynom eines Elemente $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$ ist $x^2 + x + 1$.

Jetzt kommt Ringtheorie (im Prinzip haben wir fast nur kommutative Ringe betrachtet):

1. Ringe und Ringhomomorphismen

   Beispiel. Körper, Polynomringe $R[x]$, $\mathbb{Z}$, Produkte von Ringen,...

   Homomorphismen $R[x] \to S$ sind bestimmt durch die Einschränkung auf $R \sqcup \{x\}$ (und diese setzen sich immer fort für S kommutativ).

2. Ideale $I \subseteq R$ und Quotientenring R/I. Universelle Eigenschaft: Homomorphismen $R/I \to S$ sind gegeben durch Homomrophismen $R \to S$ die I auf 0 schicken. Es gilt für $\varphi : R \to S$ dass $\mathrm{Im}(\varphi) = R/\ker(\varphi)$.

   Definition Primideal, maximales Ideal, Teilbarkeit, Primelmente, unzerlegbare Elemente

Beispiel. Kerne sind Ideale, Hauptideal $(x) = xR$ (R kommutativ), Jedes ideal ist ein Kern, Produkt und Summer von Idealen. Hauptideale (x) in Integritätsringen sind prim, wenn x prim ist.

Satz (Chinesischer Restsatz)**.** *Für teilerfremde Ideale I, J (d.h. $I + J = R$) gilt*

$$R/(I \cdot J) = R/I \times R/J$$

Beispiel. Es gilt $\mathbb{Z}/(mn) = \mathbb{Z}/m \times \mathbb{Z}/n$ für m, n teilerfremd. Es gilt $\mathbb{Q}[x]/(x^p - 1) = \mathbb{Q} \times \mathbb{Q}(\zeta_p)$ für p prim.

3. Integritätsringe, Faktorielle Ringe, Hauptidealringe, euklidische Ringe. Es gilt

   $$\text{euklidisch} \Rightarrow \text{Hauptidealring} \Rightarrow \text{Faktorielle} \Rightarrow \text{Integritätsring}$$

   In Integritätsringen sind Hauptideale das gleiche wie Elemente bis auf Einheiten. In Faktoriellen Ringen gibt es eine eindeutige Primfaktorzerlegung und eine gute Theorie von ggT's. in hauptidealringen gilt ausserdem das Lemma von Bezout (d.h. der ggT(a, b) ist Linearkombination von a und b).

   Beispiel. $\mathbb{Z}$ ist euklidisch, $K[x]$ ist euklidisch, $\mathbb{Z}[x]$ ist faktoriell, aber nicht PID.

   In Faktoriellen Ringen sind Prim und Irreduzible Elemente das Gleiche. In Hauptiealringen sind Primideale $p \neq 0$ maximal.

   Beispiel. Das gilt nicht in faktoriellen Ringen, auch nicht für Hauptideale, z.B. in $\mathbb{Z}[x]$ ist $x + 1$ irreduzibel, aber nicht maximal

4. Lemma von Gauss: für $R[x]$ faktoriell genau dann, wenn $R[x]$ faktoriell ist. Die Primelemente sind: Primelemente in R und primitive Polynome in $R[x]$ die Prim in $K[x]$ sind (K Quotientenkörper).

   Beispiel. $\mathbb{Z}[x]$ ist faktoriell. Ein primitives Polynom in $\mathbb{Z}[x]$ ist irreduzibel, genau dann wenn es in $\mathbb{Q}[x]$ irreduzibel ist. Ein nicht-primitives Polynom in $\mathbb{Z}[x]$ ist nicht irreduzibel.
   Das Polynom $\Phi_p(x) = x^{p-1} + ... + 1$ is irreduzibel in $\mathbb{Z}[x]$ also auch in $\mathbb{Q}[x]$.
   Allgemeiner sind Eisensteinpolynome aus $R[x]$ irreduzibel in $K[x]$.

5. Wir haben für $f \in K[x]$ eine (bis auf Einheiten eindeutige) Darstellung

   $$f = \text{cont}_R(f)\tilde{f} \qquad \text{cont}_R(f) \in K, \tilde{f} \in \mathbb{R}[x] \text{ primitiv}$$

   Es gilt $f \in R[x] \Leftrightarrow \text{cont}_R(f) \in R$. Ausserdem gilt

   $$\text{cont}_R(fg) = \text{cont}_R(f)\,\text{cont}_R(g).$$

   Konsequenzen: Nullstellen primitiver, ganzzahliger Polyonome sind ganzzahlig (und teilen das Absolutglied). Für $f \in R[x]$ normiert mit $f = gh$ in $K[x]$ normiert gilt $g, h \in R[x]$.

Beispiel. $\text{cont}_{\mathbb{Z}}(f) = 1/r$ für $f \in \mathbb{Q}[x]$ normiert.
Eine n-te Wurzel aus einer ganzen Zahl ist entweder ganzzahlig oder irreduzibel

Das nächste Thema sind Gruppen (und kommt noch):

11 Zerfällungskörper

Definition 11.1. *Sei $f \in K[x]$ ein Polynom. Dann heisst eine Körpererweiterung E von K ein* Zerfällungskörper *von f falls gilt:*

1. *f zerfällt über E in Nullstellen*
2. *E ist minimal bezüglich (1), d.h. es gibt keinen Zwischenkörper $K \subseteq E' \subseteq E$ sodass f bereits über E' zerfält.*

Man kann die zweite Eigenschaft auch äquivalent dadurch ausdrücken, dass $E = K(z_1, .., z_n)$ wobei $z_1, .., z_n$ die Wurzeln von f sind. Insbesondere ist E eine endliche Körpererweiterung. Wir warnen davor, dass es weniger Wurzeln als den Grad des Polynoms geben kann.

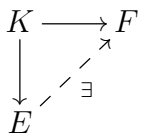
Beispiel 11.2.
1. Sei $f \in \mathbb{Q}[x]$ ein Polynom mit komplexen Nullstellen $z_1, .., z_n$. Dann ist $\mathbb{Q}(z_1, ..., z_n) \subseteq \mathbb{C}$ ein Zerfällungskörper von f.
2. $\mathbb{C}$ ist ein Zerfällungskörper von $x^2 + 1 \in \mathbb{R}[x]$.
3. $\mathbb{Q}(\zeta_n)$ ist ein Zerfällungskörper von $x^n - 1 \in \mathbb{Q}(\zeta)$.

Satz 11.3. *Für jedes Polynom $f \in K[x]$ existiert ein Zerfällungskörper.*

Proof. Wir spalten einen irreduziblen Faktor von f ab, also $f = f'g$ mit f' irreduzibel. Dann betrachten wir den Körper $E_1 := K[x]/f'$. Über diesem Körper hat f eine Nullstelle (nämlich x). Wir spalten den Linearfaktor von f über E und wiederholen die Prozedur, bis f vollständig zerfällt. □

Jetzt fragen wir uns, wie eindeutig Zerfällungskörper sind. Optimal wäre, falls der Zerfällungskörper E einer universelle Eigenschaft hätte. Leider haben wir das nicht ganz, sondern nur eine schwache Version:

Satz 11.4 (Schwache Universelle Eigenschaft des Zerfällungskörpers)**.** *Sei E ein Zerfällungskörper von f und $K \to F$ eine Körpererweiterung über der F zerfällt. Dann existiert ein Morphismus*



der aber nicht eindeutig ist.

Proof. Wir haben $E = K(\alpha_1, ..., \alpha_k)$ wobei α_i die Nullstellen von f sind. Um die Abbildung $K \to F$ über $K(\alpha)$ zu erweitern müssen wir wegen

$$K(\alpha) = K[x]/\min_K(\alpha)$$

eine Nullstelle von $\min_K(\alpha)$ in F wählen. Diese existiert aber, da $\min_K(\alpha)|f$. Wir fahren nun induktiv über alle Nullstellen fort. □

Korollar 11.5. *Je zwei Zerfällungskörper sind nicht kanonisch isomorph.*

Proof. Seien E und E' Zerfällungskörper. Dann existieren Morphismen $E \to E'$ und $E' \to E$. Da beide Körperweiterungen endich sind und die Morphismen injektiv und K-linear, folgt, dass E und E' die gleiche Dimension haben und die Morphismen Isomorphismen sind. □

Wegen dieses Satzes wird auch oft von *dem* Zerfällungskörper gesprochen. Da der Isomorphismus allerdings nicht kanonisch ist, muss man vorsichtig sein. Das ist ähnlich wie von dem Vektorraum der Dimension n zu sprechen. Zum Beispiel im Fall $K = \mathbb{Q}$ und $E = \mathbb{Q}(\zeta_n)$, dem Zerfällungskörper von $x^n - 1$ sehen wir, dass es jede Menge Automorphismen von $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ gibt, namlich $\phi(n)$-viele. Das zeigt, warum Zerfällungskörper nicht kanonisch/eindeutig sind. Wir können uns aber fragen, wie nicht-eindeutig die Fortsetzung in Satz 11.4 ist. Dazu haben wir folgendes Resultat:

Satz 11.6. *Sei E/K eine endliche Körperweiterung und F/K eine beliebige Körpererweiterung. Dann gilt*

$$|\operatorname{Hom}_K(E, F)| \leq [E : K] \ .$$

Proof. Angenommen $E = K(\alpha) = K[x]/\min_K(\alpha)$. Dann gilt

$$\operatorname{Hom}_K(E, F) \cong \{x \in F \mid \min_K(\alpha)(x) = 0\}$$

und die Ungleichung folgt, da die Anzahl der Nullstellen durch den Grad des Polynoms und damit den Grad $[E : K]$ beschränkt ist.
Anderenfalls finden wir einen echten Zwischenkörper $K \subseteq K(\alpha) \subseteq E$ und wir nehmen per Induktion über den Grad an, dass die Behauptung für die Erweiterung $E/K(\alpha)$ bereits gezeigt ist. Dann haben wir

$$\begin{aligned}
|\operatorname{Hom}_K(E, F)| &= |\coprod_{\operatorname{Hom}_K(K(\alpha),F)} \operatorname{Hom}_{K(\alpha)}(E, F)| \\
&= \sum_{\operatorname{Hom}_K(K(\alpha),F)} |\operatorname{Hom}_{K(\alpha)}(E, F)| \\
&\leq \sum_{\operatorname{Hom}_K(K(\alpha),F)} [E : K(\alpha)] \\
&= |\operatorname{Hom}_K(K(\alpha), F)|[E : K(\alpha)] \\
&\leq [K(\alpha) : K] \cdot [E : K(\alpha)] = [E : K]
\end{aligned}$$

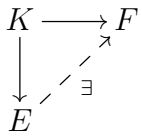
□

Wir können nun auch für eine Familie von Polynomen Zerfällungskörper betrachten:

Definition 11.7. *Für eine Teilmenge $S \subseteq K[x]$ heisst eine Körpererweiterung E/K ein Zerfällungskörper von S falls alle Polynome $f \in S$ über E zerfallen und E minimal mit dieser Eigenschaft ist (äquivalent: E wird von den Nullstellen aller Polynome in S erzeugt).*

Bemerkung 11.8. Falls S aus einem Element besteht sind wir im vorherigen Fall. Fall S endlich ist, so können wir das produkt $f = \prod_S s$ bilden. Dann ist E Zerfällungskörper von f genau dann, wenn es Zerfällungskörper von S ist. Somit sind wir wieder im bisherigen Fall und wir wissen, dass der Zerfällungskörper existiert und eine schwache universelle Eigenschaft besitzt. Wir wollen nun beweisen, dass dies auch für eine beliebige Teilmenge S geht.

Satz 11.9. *Für jede Familie $S \subseteq K[x]$ existiet ein Zerfällungskörper E. Dieser hat die schwache universelle Eigenschaft, dass für jede Körpererweiterung $K \to F$ über der alle Polynome aus S zerfallen eine Morphismus*



existiert.

Wir werden diesen Satz im nächsten Kapitel beweisen. Bis dahin ziehen wir zunächst Konsequenzen. Aber die Beweisidee wollen wir kurz skizzieren:

Beweisidee von Satz 11.9. Wir nehmen zunächst an, dass die Menge $S \subseteq K[x]$ abzählbar ist und numerieren sie:

$$f_1, f_2, f_3, ...$$

Wir bilden einen Zerfällungskörper E_1 von f_1. Anschliesend einen Zerfällungskörper von f_2 über E_2 etc.
Auf diese Weise erhalten wir einen Turm

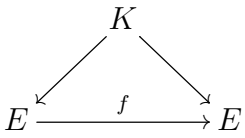
$$K \to E_1 \to E_2 \to E_3 \to ...$$

sodass über E_k alle Polynome $f_1, ..., f_k$ zerfallen, und E_k de facto der Zerfällungskörper dieser Polynome ist. Dann ist der gesuchte Körper die Vereinung dieser Körper E_i. Dieser Term macht gerade keinen Sinn und wir werden im kommenden Kapitel erläutern was wir damit meinen. □

Korollar 11.10. *Je zwei Zerfällungskörper E und E' von S sind nicht kanonisch isomorph.*

Proof. Wir haben Abbildungen $f : E \to E'$ und $g : E' \to E$. Dann sind die Kompositionen $gf : E \to E$ und $E' \to E'$ Endomorphismen. Es reicht zu zeigend, dass gf und fg Isomorphismen sind (warum?). Das folgt aus dem nächsten Lemma. □

Lemma 11.11. *Sei E/K eine algebraische Körpererweiterung. Dann ist jeder Körperendomorphismus $f : E \to E$ über K (d.h. das Diagram*



ein Isomorphismus.

Proof. f ist injektiv, da es ein Körperhomomorphismus ist. Wir müssen also zeigen, dass es auch surjektiv ist. Dazu sei $e \in E$ Nullstelle des Polynoms $f \in K[x]$. Offensichtlich induziert f eine Abbildung

$$\{\text{Nullstellen von } f \text{ in } E\} \to \{\text{Nullstellen von } f \text{ in } E\ \}$$

Diese Abbildung ist injektiv (da f injektiv ist) und daher auch surjektiv, da die Menge endlich ist. Also liegt e im Bild von f. □

Bemerkung 11.12. Für nicht algebraische Körpererweiterungen ist das Lemma falsch. So gibt es Beispielsweise die Abbildung

$$\mathbb{Q}(x) \to \mathbb{Q}(x) \qquad x \mapsto x^2$$

welche nicht surjektiv ist, da zum Beispiel x nicht im Bild liegt.

12 Zerfällungskörper als gerichtete colimits

Definition 12.1. *Eine gerichtete Menge ist eine Menge I zusammen mit einer Relation $\leq$ die Reflexiv und Transitiv und Antisymmetrisch ist (also eine geordnete Menge) sodass für jedes Paar $i, j \in I$ eine obere Schranke existiert, d.h. ein Element $k \in I$ exisitert mit $i \leq k$ und $j \leq k$. Wir schreiben $i < j$ falls $i \leq j$ und $i \neq j$.*

Beispiel 12.2. Die Menge $(\mathbb{N}, \leq)$ ist gerichtet. Ebenso die Menge $\mathbb{N}_{\leq n} = \{0, 1, 2, ..., n\}$. Allgmeiner ist jede total geordnete Menge gerichtet, wobei total geordnet heisst, dass für a, b gilt $a \leq b$ oder $b \leq a$.

Beispiel 12.3. Sei I eine beliebige Menge. Wir können auf I eine Wohlordnung wählen (nach dem Wohlordnungssatz, welcher äquivalent zum Auswahlaxiom ist), d,h. eine Relation $\leq$ sodass jede nicht-leere Teilmenge $I_0 \subseteq I$ ein bezüglich $\leq$ minimales Element besitzt und sodass $\leq$ eine totale Ordnung ist. Insbesondere ist $(I, \leq)$ dann gerichtet.
In einer wohlgeordneten Menge I hat ausserdem jedes Element $i \in I$ einen Nachfolger: betrachte einfach die Menge $\{j \in I \mid j > i\}$. Diese hat ein minimales Element, welches wir den Nachfolger von i nennen. Es gibt aber im Allgemeinen keinen Vorgänger: zum Beispiel in $\mathbb{N}$ hat die 0 keinen Vorgänger oder in $\mathbb{N} \sqcup \{\infty\}$ hat ∞ keinen Vorgänger (aber die Mengen sind wohlgeordnet).

Definition 12.4. *Für eine gerichtete Menge sei für jedes $i \in I$ ein Körper gegeben und für jedes Paar (i,j) mit $i < j$ einen Morphismus $\varphi_{ij} : K_i \to K_j$ sodass für $i < j < k$ die Komposition*

$$\varphi_{jk} \circ \varphi_{ij} : K_i \to K_j \to K_k$$

gleich φ_{ik} ist. Manchmal setzen wir auch $\varphi_{ii} = \mathrm{id}_{K_i}$ sodass φ_{ij} für $i \leq j$ definiert ist. Eine solche Familie von Körpern und Körpermorphismen bezeichnen wir als I-indiziertes Diagram von Körpern (oder kurz gerichtetes Diagram).

Beispiel 12.5. Sei $I = (\mathbb{N}, \leq)$. Dann ist ein I-indiziertes Diagram gegeben durch ein Diagram

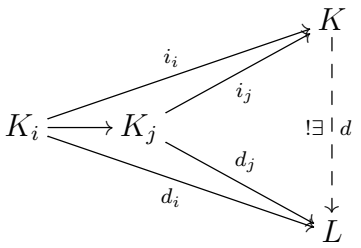
$$K_0 \to K_1 \to K_2 \to K_3 \to ...$$

Die Abbildungen sind alle injektiv, können wir also als Inklusionen auffassen. Was wir jetzt im Folgenden machen wollen ist abstrakt eine "Vereinigung" der K_i zu definieren. Die Idee, die wir im Folgenden beweis präzisieren wollen ist diese zu definieren als Quotient von

$$\coprod K_i$$

zu definieren, wo wir K_i mit seinem Bild in K_{i+1} identifizieren.

Definition 12.6. *Für eine gerichtetes Diagram (K_i, φ_{ij}) von Körpern heisst ein Körper K zusammen mit Abbildungen $i_i : K_i \to K$ sodass $i_j \circ \varphi_{ij} = i_i$ (gerichteter)* Kolimes*, falls für jeden weiteren Körper L und jede Familie von Abbildungen $d_i : K_i \to L$ mit $d_j \circ \varphi_{ij} = d_i$ genau eine Abbildung $d : K \to L$ existiert sodass $d_i = d \circ i_i$*



Wir schreiben dann $K = \varinjlim_i K_i$.

Beispiel 12.7. Sei ein Körper K gegeben mit Unterkörpern

$$K_1 \subseteq K_2 \subseteq K_3 \subseteq ... \qquad \subseteq K$$

sodass $K = \bigcup K_i$. Dann ist K der Kolimes der K_i. Denn ein Morphismus $K \to K$ ist durch die Restriktionen auf die K_i bestimmt, genauer

Beispiel 12.8. Angenommen I besitzt ein maximales Element $i_0 \in I$. Dann ist $K_i = \varinjlim K_i$.

Satz 12.9. *Für jedes gerichtete Diagram von Körpern existiert ein gerichteter Kolimes. Dieser ist eindeutig bis auf eindeutige Isomorphie.*

Proof. Wir definieren die unterliegende Menge des Körpers K als

$$K := \coprod_{i \in I} K_i / \sim$$

wobei $\sim$ die Äquivalenzrelation ist die erzeugt ist von

$$k \in K_i \sim \varphi_{ij}(k) \in K_j \ .$$

für $i < j$. Erzeugt meint hierbei, dass es die kleinste Äquivalenzrelation ist, sodass die gegebenen Relationen erfüllt sind. Die gegebene Relation is zum Beispiel nicht symmetrisch und reflexiv, also erzwingen wir das.
Wir wollen nun K zu einem Körper machen. Dazu definieren wir eine Addition und Multiplikation von Klassen $[x]$ und $[y]$ wie folgt: die Repräsentanten liegen in $x \in K_i$ und $y \in K_j$. Wir wählen $i \leq k$ und $j \leq k$ und können x durch $\varphi_{ik}(x)$ erzetzen und y durch $\varphi_{jk}(y)$ sodass wir oBda annehmen können, dass $i = j$. Dann definieren wir

$$[x] + [y] := [x + y] \ .$$

Dies ist wohldefiniert, weil für $k \leq k'$ gilt, dass $\varphi_{kk'}$ Addition erhält. Mit dem exakt gleichen Trick definieren wir die Multiplikation. Die 0 und die 1 sind gegeben durch $[0], [1]$ mit $0, 1 \in K_i$ für irgendein i. Um zu sehen, dass K ein Körper ist, stellen wir fest, dass jede nachzurechnende Gleichung endloch viele Elemente enthält und wir wiederum oBdA annehmen können, dass sie alle in einem Körper liegen. Inverse sind ebenfalls einfach.
Wir definieren nun die Abbildungen

$$i_i : K_i \to K \qquad x \mapsto [x]$$

und diese sind Körperhomomorphismen per Definition.
Für die universelle Eigenschaft sei ein ...
Die eindeutigkeit □

Beispiel 12.10. Wir betrachten wieder den Fall $K_1 \to K_2 \to K_3 \to ...$ von Körperhomomorphismen und bezeichnen den Kolimes mit K. Dann können wir mittels i_i den Körper K_i als Teilmenge $K_i' := i_i(K_i)$ bezeichnen. Wir haben dann, dass

$$K_1' \subseteq K_2' \subseteq K_3' \subseteq ... \qquad \subseteq K$$

Dann ist $K = \cup K_i'$. Dies ist gewissermaßen die Umkehrung von Beispiel 12.7.

Beispiel 12.11. Sei E/K eine Körpererweiterung erzeugt von abzählbar vielen Elementen $\alpha_1, \alpha_2, \alpha_3, ...$ Dann ist E der Kolimes der

$$K_i := K(\alpha_1, ..., \alpha_i) \subseteq K$$

Falls E von einer beleibigen Menge α_i mit $i \in I$ erzeugt ist so wählen wir eine Wohlordnung auf I (totale Ordnung, sodass jede nicht-leere Teilmenge ein Minimum besitzt). Wir definieren jetzt induktiv für jedes $i \in I$ einen Körper wie folgt:

1. Für das Minimum $i \in I$ setzen wir $K_i := K(\alpha_i)$.
2. Für allgemeines $i \in I$ setzen wir

$$K_i := \left(\varinjlim_{j<i} K_j\right)(\alpha_i)$$

Wir bemerken, dass falls $i \in I$ der Nachfolger von $i' \in I$ ist gilt, dass

$$\left(\varinjlim_{j<i} K_j\right)(\alpha_i) = K_{i'}(\alpha_i)$$

Daher stimmt dies mit der Definition die wir oben gegeben haben über ein. Für $i < j$ haben wir eine kanonische Inklusion $K_i \to K_j$. Nun haben wir, dass

$$K = \varinjlim_i K_i \ .$$

Jetzt wollen wir Satz 11.9 beweisen. Zur Erinnerung nochmal das Statement:

Satz. *Für jede Familie $S \subseteq K[x]$ existiet ein Zerfällungskörper E. Dieser hat die schwache universelle Eigenschaft, dass für jede Körpererweiterung $K \to F$ über der alle Polynome aus S zerfallen eine Morphismus*

$$\begin{array}{ccc} K & \longrightarrow & F \\ \downarrow & \nearrow_{\exists} & \\ E & & \end{array}$$

existiert.

Zunächst beweisen wir die Existenzaussage. Diese folgt sofort aus dem folgenden Lemma:

Lemma 12.12. *Sei $E = K(a_i \mid i \in I)$ für I erzeugt von algebraischen Elementen. Für eine Körpererweiterung F/K existiert dann eine Abbildung $E \to F$ über K falls alle Minimalpolynome von a_i über E zerfallen.*

Proof. Nach dem vorigen Beispiel 12.11 ist $E = \varinjlim K_i$ also um eine Abbildung $E \to F$ zu definieren müssen wir induktiv Abbildungen $K_i \to F$ definieren. Dazu müssen wir nach Definiton

$$K_i = \left(\varinjlim_{j<i} K_j\right)(\alpha_i) = \left(\varinjlim_{j<i} K_j\right)[x]/\min(\alpha)$$

die Abbildungen auf definieren. Induktiv haben wir bereits die Abbildungen auf K_j definiert sodass es ausreicht ein Bild für α zu finden. Das können wir aber, da das Minimalpolynom von α relativ zu $\left(\varinjlim_{j<i} K_j\right)$ ein Teiler des Minimalpolynoms relativ zu K ist und daher eine Nullstelle hat. □

Nun kommen wir zur Exisenzaussage:

Beweis Satz 11.9. Zunächst vervollständigen wir die Beweisidee: dazu nehmen wir wieder an, dass die Menge $S \subseteq K[x]$ abzählbar ist und numerieren sie:

$$f_1, f_2, f_3, ...$$

Wir bilden einen Zerfällungskörper E_1 von f_1. Anschliesend einen Zerfällungskörper von f_2 über E_2 etc.
Auf diese Weise erhalten wir einen Turm

$$K \to E_1 \to E_2 \to E_3 \to ...$$

sodass über E_k alle Polynome $f_1, ..., f_k$ zerfallen, und E_k de facto der Zerfällungskörper dieser Polynome ist. Dann ist der gesuchte Körper der Kolimes der E_i. Dieser erfüllt dann alle Eigenschaften.
Nun zu beliebigem S: wir wählen eine Wohlordnung auf S und definieren induktiv Körper E_s. Für das Minimum $s \in S$ definieren wir E_s als einen Zerfällungskörper von s über K. Für beliebiges $s \in S$ setzen wir E_s als Zerfälllungskörper von s über $\varinjlim_{s'<s} E_{s'}$. Dann ist $E := \varinjlim_s E_s$ der gesuchte Zerfällungskörper. □

13 Algebraischer Abschluss

In diesem Kapitel wollen wir den Zerällungskörper alles Polynome $K[x]$ näher untersuchen. Es wird sich zeigen, dass dies der algebraische Abschluss ist.

Definition 13.1. *Ein Körper E heisst algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom $f \in E[x]$ eine Nullstelle hat.*

Beispiel 13.2.
1. Die komplexen Zahlen sind algebraisch abgeschlossen. Der Beweis benötigt aber nicht-algebraische Hilfsmittel (z.B. Funktionentheorie mittels der Tatsache, dass jede analytische Abbildung offen ist).

2. Keiner der Körper $\mathbb{Q}, \mathbb{R}$ ist algebraisch abgeschlossen, da das Polynom $x^2 + 1$ keine Nullstelle hat.

3. Die Körper $\mathbb{F}_p$ für p prim sind nicht algebraisch abgeschlossen, zum Beispiel hat $x^p - x + 1$ keine Nullstelle, da nach dem Satz von Lagrange gilt $x^p = x$ für jedes $x \in \mathbb{F}_p$.

Definition 13.3. *Eine Körpererweiterung E/K heisst ein* algebraischer Abschluss *von K falls sie algebraisch ist und E algebraisch abgeschlossen ist.*

Beispiel 13.4. $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$.

Unser Ziel ist es nun zu zeigen, dass für jeden Körper ein algebraischer Abschluss existiert. Unser Kandidat ist der Zerfällungskörper E aller Polynome in $K[x]$. Darüber zerfallen alle Polynome aus $K[x]$ in Linearfaktoren. Es könnte aber neue Polynome in $E[x][$ geben, die nicht aus $K[x]$ stammen und nicht zerfallen. Wir werden nun sehen, dass das nicht passieren kann:

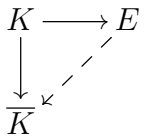
Lemma 13.5. *Sei E/K algebraisch mit der Eigenschaft, dass jedes Polynom aus $K[x]$ über E zerfällt. Dann ist E bereits algebraisch abgeschlossen und somit ein algebraischer Abschluss von K.*

Proof. Sei $f \in E[x]$. Wir bilden einen Zerfällungskörper E' von f über E. Dann ist E'/E algebraisch und damit auch E'/K (Korollar 3.13). Insbesondere ist jedes Element $e \in E'$ Nullstelle eines Polynoms über K und damit bereits in E enthalten. □

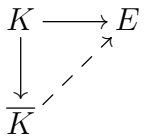
Beispiel 13.6. Über dem Körper $\overline{\mathbb{Q}}$ der algerbaischen Elemente zerfällt jedes Polynom aus $\mathbb{Q}$. Also ist $\overline{\mathbb{Q}}$ algerbaisch abgeschlossen und somit ein algebraischer Abschluss von $\mathbb{Q}$. Wir bemerken, dass $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, denn falls dieser Grad gleich $n < \infty$ wäre so müsste jedes irreduzible Polynom über $\mathbb{Q}$ Grad $\leq n$ haben. Aber $x^k - 2$ ist nach Eisenstein für jedes k irreduzibel. Wir sehen, dass der algebraische Abschluss auch unendlichen Grad haben kann (aber immernoch algebraisch ist).

Satz 13.7. *Für jeden Körper K existiert ein algebraischer Abschluss $\overline{K}$. Dieser hat die folgenden beiden schwachen universelle Eigenschaften:*

1. *Für jede algebraische Körpererweiterung E/K existiert ein Morphismus*



2. *Für jede Körpererweiterung E/K über der alle Polynome aus $K[x]$ in Linearfaktoren zerfallen (zum Beispiel wenn E selbst algebraisch abgeschlossen ist) existiert ein Morphismus*



Je zwei algebraische Abschlüsse sind nicht-kanonisch isomorph.

Proof. Das vorherige Lemma zeigt, dass jeder Zerfällungskörper von $K[x]$ ein algebraischer Abschluss ist. Umgekehrt ist jeder algebraische Abschluss E auch ein Zerfällungskörper von $K[x]$, da jedes Polynom aus $K[x]$ über E zerfällt und jedes Element aus E algebraisch über K ist, also Nullstelle eines Polynoms aus $K[x]$. Daraus folgt bereits alles bis auf die erste universelle Eigenschaft. Um diese zu beweisen sei E/K algebraisch. Wir bilden einen algebraischen Abschluss $\overline{E}$, welcher nach dem bisher gezeigten existiert. Dann ist $\overline{E}$ aber algebraisch über K (transitivität) und daher auch ein algebraischer Abschluss von K, insbesondere gibt es einen iMorphismus

$$E \subseteq \overline{E} \xrightarrow{\simeq} \overline{K}$$

über K. □

Beispiel 13.8. Wir haben den algebraischen Abschluss als Zerfällungskörper realisiert. Sei umgekehrt $\overline{K}$ ein algebraischer Abschluss von K. Wir können für jede Teilmenge $S \subseteq K[x]$ von Polynomen einen Zerfällungskörper E als Unterkörper von $\overline{K}$ bekommen, indem wir die Nullstellen aller Polynome aus S an K adjungieren (in $\overline{K}$). Für jeden anderen Zefällungskörper E' und jede Abbildung $f : E' \to \overline{K}$ über K (die existiert) stimmt dann das Bild $f(E) \subseteq \overline{K}$ mit E überein. Das liegt daran, dass die Abbildung höchtens die Nullstellen jeder Polynomes in S permutiert.
Mit anderen Worten: wenn wir einen algebraischen Abschluss E von K fixieren sind Zerfällungskörper als Unterkörper von $\overline{K}$ eindeutig.

Korollar 13.9. *Sei $f : K \to K$ ein Körperendomorphismus und $\overline{K}$ ein algebraischer Abschluss. Dann kann man f zu einem Endomrohpismus $\overline{K} \to \overline{K}$ fortsetzen.*

Proof. Betrachte die Komposition $K \xrightarrow{f} K \to \overline{K}$. Nach der ersten universellen Eigenschaft können wir diese fortsetzen. □

Beispiel 13.10. Dies hat verrückte Konsequenzen. Zum Beispiel können wir jede Menge Körperautomorphismen von $\overline{\mathbb{Q}}$ konstruieren: wir nehmen beispielsweise einen Automorphimus $\mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p)$ und setzen ihn zu $\overline{\mathbb{Q}}$ fort!

Wir können uns nun fragen, ob wir einer Körpererweiterung E/K ansehen können, dass sie Zerfällungskörper einer Familie von Polynomen $S \subseteq K[x]$ ist.

Definition 13.11. *Eine Körpererweiterung E/K heisst* normal*, falls jedes irreduzible Polynom $f \in K[x]$ welches eine Nullstelle in E hat bereits über E in Linearfaktoren zerfällt.*

Beispiel 13.12. Die Erweiterung $E = \mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ ist nicht normal über $\mathbb{Q}$, denn das irreduzible Polynom $x^3 - 2 \in \mathbb{Q}[x]$ hat die Nullstelle $\sqrt[3]{2}$ aber zerfällt nicht (da die anderen Nullstellen nicht reell sind).

Satz 13.13. *Eine algebraische Körpererweiterung E/K ist genau dann Zerfällungskörper einer Familie von Polynomen, wenn sie normal ist.*

Proof. Angenommen E ist normal und $E = K(\alpha_i \mid i \in i)$ für algebraische Elemente $\alpha_i \in E$. Solche existieren stets, im Zweifelsfall kann man alle Elemente aus E nehmen oder eine K-basis von E. Wir betrachten die Menge $S = \{\min_K(\alpha_i) \mid i \in I\} \subseteq K[x]$. Dann ist E ein Zerfällungskörper von S, denn die Polynome $\min_K(\alpha_i)$ haben nach Konstruktion eine Nullstelle in E, zerfallen also auch.
Umgekehrt sei E/K ein Zerfällungskörper von $S \subseteq K[x]$. Nun sei $f \in K[x]$ irreduzibel und angenommen f hat eine Nullstelle $\alpha \in E$. Sei $\overline{E}$ ein algebraischer Abschluss (eine Zerfällungskörper von f über E würde es auch tun, falls man das Auswahlaxiom vermeiden möchte). Für jede Nullstelle β von f in $\overline{E}$ gibt es einen Morphismus

$$K(\alpha) \to \overline{E} \qquad \alpha \mapsto \beta$$

über K. Diesen können wir zu einem Morphismus

$$\psi : E \to \overline{E}$$

fortsetzen, nach der schwachen Universellen Eigenschaft. Insbesondere stimmt das Bild $\psi(E)$ mit E überein (nach Beispiel 13.8). Damit liegt aber β auch in E. □

Bemerkung 13.14. Es folgt, dass endliche normale Körpererweiterungen genau die Zerfällungskörper eines einzelnen Polynoms sind.

14 Primkörper und Charakteristik

Definition 14.1. *Ein Körper heisst Primkörper, wenn er keinen echten Teilkörper enthält. Der Primkörper eine beliebigen Körpers ist der eindeutig bestimmte Primkörper der Teilkörper von K ist. Er ist gleich dem Durchschnitt aller Teilkörper.*

Beispiel 14.2.

1. Die Körper $\mathbb{Q}$ und $\mathbb{F}_p$ sind prim.
2. Für jeden Körper K betrachten wir den Homomorphismus $\mathbb{Z} \to K$. Dieser hat als Kern ein Primideal, also entweder $p\mathbb{Z}$ oder 0. Im ersten Fall gilt $\mathbb{F}_p \subseteq K$ und im zweiten $\mathbb{Z} \subseteq K$ und damit $\mathbb{Q} \subseteq K$.[5] Wir sagen im ersten Fall, dass K Charakteristik p hat ($\mathrm{Char}(K) = p$) und im zweiten, dass K Charakteristik 0 hat ($\mathrm{Char}(K) = 0$).
3. Das zeigt auch, dass $\mathbb{F}_p$ und $\mathbb{Q}$ die einzigen Primkörper sind. Ausserdem folgt, dass für einen Körperhomomorphismus $K \to K'$ gilt $\mathrm{Char}(K) = \mathrm{Char}(K')$.

Wir wollen nun den Begriff der Charakteristik auch auf Ringe ausweiten. Das diskutieren wir nun ein wenig. Der Einfachheit halber besprechen wir nur kommutative Ringe.

Definition 14.3. *Sei R ein kommutativer Ring. Wir definieren die Characteristic von R als die kleinste Zahl n sodass $n = 0$ in R gilt falls eine solche existiert und 0 sonst und bezeichnen sie mit* $\mathrm{Char}(R)$.

Beispiel 14.4. Es gilt $\mathrm{Char}(\mathbb{Z}) = \mathrm{Char}(\mathbb{Q}) = 0$ und $\mathrm{Char}(\mathbb{Z}/n) = n$.

Das Problem ist, dass dieser Begriff der Charkateristik keine Primzahl ist. Das kann man korrigieren. Es sei $\mathbb{P} = \{2, 3, 5, ...\}$ die Menge aller Primzahlen und $\overline{\mathbb{P}} = \mathbb{P} \coprod \{0\}$ die Vereinigung mit 0.

Definition 14.5. *Der Support ist definiert als Teilmenge von $\overline{\mathbb{P}}$ durch*

$$\mathrm{Supp}(R) := \{\mathrm{Char}(\mathrm{Quot}(R/p)) \mid p \subseteq R \text{ Primideal}\} .$$

Beispiel 14.6.

1. Für einen Körper K sind die Definitionen konsistent, denn er besitzt nur ein einziges Primideal, sodass $\mathrm{Supp}(K) = \{\mathrm{Char}(K)\}$.

[5] Sloppy Notation.

2. Der Support von $\mathbb{Z}$ ist $\overline{\mathbb{P}}$.

3. Der Support von $\mathbb{Z}/n$ ist die Menge aller Primteiler von n.

Äquivalent zur Definition haben wir

$$\mathrm{Supp}(R) = \{\mathrm{Char}(K) \mid R \to K \text{ Ringhom mit } K \text{ Körper}\}$$

Dies folgt daraus, dass für jeden solchen Homomorphismus $R \to K$ der Kern einprimideal $I = \ker$ ist und somit eine Faktorisierung

$$R \to \mathrm{Quot}(R/I) \to K \ .$$

existiert.

Proposition 14.7. *Für jeden Ringhomomorphismus $R \to S$ gilt* $\mathrm{Supp}(S) \subseteq \mathrm{Supp}(R)$.

Proof. Klar, denn für jeden Homomorphismus $S \to K$ in einen Körper existiert somit auch ein Homomorphismus $R \to S \to K$. □

Lemma 14.8. *Angenommen R ist kommutativ und $I \subseteq R$ ist ein Ideal mit $I \neq R$. Dann existiert ein maximales Ideal $I \subseteq \mathfrak{m} \subseteq R$. Insbesondere hat jeder nicht-trviale kommutiative Ring maximale Ideale.*

Proof. Wir benutzen Zorn's Lemma, welche eine Aussage der Logik ist die äquivalent zum Auswahlaxiom ist:

> Sie P ein geordnete Menge mit der Eigenschaft, dass jede total geordnete Teilmenge $S \subseteq P$ eine obere Schranke in P besitzt. Dann existiert in P für jedes Element $p \in P$ ein maximales Element $p \leq m$.

Wir wenden dies hier an auf die Menge der Ideale $I \subseteq R$ mit $I \neq R$ (äquivalent $1 \notin I$). Diese ist bezüglich Inklusion geordnet und für jede total geordnete Teilmenge von Idealen ist die Vereinigung eine obere Schranke, da die Vereinigung ein Ideal ist und 1 nicht enthält. □

Satz 14.9. *1. Angenommen es gilt* $\mathrm{Supp}(R) = \{0\}$. *Dann ist* $\mathbb{Q} \subseteq R$.

2. Angenommen $\mathrm{Char}(R) = n > 1$. *Dann gilt* $\mathrm{Supp}(R) = \{$*Primteiler von* $n\}$.

3. Angenommen $\mathrm{Char}(R) = 0$. *Dann gilt* $0 \in \mathrm{Supp}(R)$.

Proof. Angenommen $\mathrm{Char}(R) = \{0\}$. Wir betrachten den Homomorphismus $\mathbb{Z} \to R$. Es kann nicht sein, dass der Kern ein $n > 0$ ist, da sonst $\mathrm{Char}(R) \subseteq \mathrm{Char}(\mathbb{Z}/n)$ gelten müsste was nicht die 0 enthält. Also ist $\mathbb{Z} \subseteq R$. Wir behaupten, dass sogar jedes Element $n \in \mathbb{Z} \subseteq R$ eine Einheit ist, was den ersten Teil beweisen würde. Also angenommen $n \in \mathbb{Z}$ ist keine Einheit in R. Dann ist $(n) \subseteq R$ ein Ideal $\neq R$ und damit in einem maximalen Ideal m enthalten. Es folgt, dass in R/m gilt $n = 0$ und somit $\mathrm{Char}(R/m)$ ein Teiler von n im Widerspruch dazu, dass kein Teiler von n in $\mathrm{Char}(R)$ enthalten sein kann. □

Beispiel 14.10. Falls $\mathrm{Supp}(R) = \{p\}$ für p prim, dann folgt *nicht*, dass $\mathbb{F}_p \subseteq R$ gilt. Zum Beispiel hat $\mathbb{Z}/p^2$ diese Eigenschaft.

Bemerkung 14.11. Man könnte für einen kommutativen Ring R auch noch einen Begriff einführen, der die beiden betrachteten Begriffe von Charakteristik kombiniert, nämlich

$$\mathrm{sChar}(R) = \{\mathrm{Char}(S) \mid R \to S \text{ ein Ringhomomorphismus } \} \subseteq \mathbb{N}$$

Dann gilt offensichtlich $\mathrm{Char}(R) \in \mathrm{sChar}(R)$ und $\mathrm{Supp}(R) \subseteq s\,\mathrm{Char}(R)$. Diese Charakteritik hat ähnliche Eigenschaften wie $\mathrm{Supp}(R)$ aber enthält mehr Information, zum Beispiel für $\mathbb{Z}/p^2$ ist sie gegeben durch $\{1, p, p^2\}$.

15 Endliche Körper

Satz 15.1. *Die Kardinalität eines endlichen Körpers ist eine Primzahlpotenz. Für jede Primzahlpotenz existiert bis auf (nicht-kanonische) Isomorphie genau ein endlicher Körper $\mathbb{F}_{p^n}$.*

Proof. Sei K ein endlicher Körper der Kardinalität q. Dann gilt $\mathbb{F}_p \subseteq K$ für p prim und somit ist K ein endlich-dimensionaler $\mathbb{F}_p$-Vektorraum und damit $q = p^n$. Nun gilt nach Lagrange angewendet auf die Multiplikative Gruppe $K^\times$, dass für jedes $x \in K^\times$ gilt $x^{q-1} = 1$. Also für jedes $x \in K$ gilt $x^q - x = 0$. Wir behaupten, dass K sogar der Zerfällungskörper von $x^q - x \in \mathbb{F}_p[x]$ ist. Dazu stellen wir fest, dass das Polynom über K genau q Nullstellen hat, also vollständig zerfällt (und der Körper offensichtlich auch von den Nullstellen erzeugt wird).
Damit wissen wir, dass je zwei Körper der Charakteristic q als Zerfällungskörper nicht-kanonisch isomorph sind. Um die Existenz zu zeigen betrachten wir einen Zerfällungskörper K von $x^q - x$ über $\mathbb{F}_p[x]$. Weil $(-)^q : K \to K$ eine Komposition des Frobenius mit sich selbst ist, ist es ein Homomorphismus und daher ist die Menge

$$K' = \{x \in K \mid x^q = x\} \subseteq K$$

ein Unterkörper der alle Nullstellen des Polynoms enthält. Also gilt $K = K'$ wegen der definierenden Eigenschaft eines Zerfällungskörpers. Ausserdem behaupten wir, dass das Polynom $f(x) = x^q - x \in K[x]$ keine mehrfachen Nullstellen haben kann (sodass K die richtige Anzahl an Elementen enthält). Dazu reicht es nach Proposition 10.11 zu zeigen, dass f und f' teilerfremd sind. Es gilt aber, dass $f'(x) = 1$. □

Die Schreibweise $\mathbb{F}_{p^n}$ ist etwas problematisch, da Zerfällungskörper nicht eindeutig sind. Was wir machen ist, dass wir einen algebraischen Abschluss $\overline{\mathbb{F}_p}$ fixieren. Dann kann man $\mathbb{F}_{p^n}$ eindeutig als Teilmenge davon realisieren, nämlich

$$\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\} \ .$$

Insbesondere folgt, dass $\overline{\mathbb{F}_p}$ unendlich viele Elemente hat (abzählbar viele, da es nur abzählbar viele Polynome über $\mathbb{F}_p$ gibt). Auf die Art haben wir Inklusionen

$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{n+1}} \subseteq ...$$

(aber nochmal: das ist nicht-kanonisch und hängt von der Wahl von $\overline{\mathbb{F}_p}$ ab). Wir behaupten, dass dann $\overline{\mathbb{F}_p}$ die Vereinigung der $\mathbb{F}_{p^n}$ ist. Dazu betrachten wir $x \in \overline{\mathbb{F}_p}$. Weil x algebraisch über $\mathbb{F}_p$ ist liegt es in einem endlichen Zwischenkörper $\mathbb{F}_p(x) \subseteq \overline{\mathbb{F}_p}$. Damit muss dann aber $x^q = x$ gelten und somit liegt x in der Vereinigung. Umgekehrt bedeutet das auch, dass wir, wenn wir für jedes n eine Wahl von $\mathbb{F}_{p^n}$ treffen und Abbildungen $\mathbb{F}_{p^n} \to \mathbb{F}_{p^{n+1}}$ wählen (die existieren nach eben gesagten) den algebraischen Abschluss als kolimes wählen können.

Es bleibt also nur noch untersuchen, wie nicht-kanonisch ein endlicher Körper $\mathbb{F}_q$ ist. Dazu muss man die Automorphismen von $\mathbb{F}_q$ untersuchen. Für jeden endlichen Körper $\mathbb{F}_q$ mit $q = p^n$ gibt es den Frobenius

$$\varphi_p : \mathbb{F}_q \to \mathbb{F}_q \qquad x \mapsto x^p$$

welcher ein Körperautomorphismus ist. Weiterhin gilt in $\mathbb{F}_q$, dass

$$(\varphi_p)^n(x) = (\varphi_p \circ ... \circ \varphi_p)(x) = ((x^p)^p)... = x^{p^n} = \mathrm{id}$$

Ausserdem ist die n die kleinste Zahl für die $\varphi_p^n = \mathrm{id}$ gilt (da wir sonst zu wenige Elemente in $\mathbb{F}_q$ hätten). Damit bekommen wir einen Inkjektiven Gruppenhomomorphismus

$$\mathbb{Z}/n \to \mathrm{Aut}(\mathbb{F}_q) \qquad 1 \mapsto \varphi_p$$

Proposition 15.2. *Für einen endlichen Körper $\mathbb{F}_q$ mit $q = p^n$ Elementen ist die Abbildung*

$$\mathbb{Z}/n \to \mathrm{Aut}(\mathbb{F}_q) \qquad 1 \mapsto \varphi_p$$

ein Isomorphismus.

Proof. Wir wissen aus Satz 11.6, dass die Menge $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Hom}(\mathbb{F}_q, \mathbb{F}_q)$ höchstens n-Elemente enthält. Also muss die obige Abbildung ein Iso sein. □

Wir können auch noch eine Aussage über Homomorphismen zwischen verschiedenen endlichen Körpern machen. Zunächst ist es klar, dass es einen Homomorphismus von $\mathbb{F}_q \to \mathbb{F}_{q'}$ nur dann geben kann, wenn $q = p^n$ und $q = p^m$ mit $m \geq n$ ist. In diesem Fall haben wie auch schon gesehen, dass es stets einen Homomorphismus gibt. In dem Fall gilt:

Proposition 15.3. *Für je zwei Homomorphismen $f, g : \mathbb{F}_q \to \mathbb{F}_{q'}$ gilt, dass genau ein $[k] \in \mathbb{Z}/n$ existiert, sodass*

$$g = f \circ \varphi_p^k = \varphi_p^k \circ f \qquad \textit{also} \qquad g(x) = f(x^{p^k}) = f(x)^{p^k}$$

Mit anderen Worten: wir haben wir für einen fixierten Homomorphismus f die Gleichheit

$$\mathrm{Hom}(\mathbb{F}_q, \mathbb{F}_{q'}) = \{f, f \circ \varphi_p, f \circ \varphi_p^2, ..., f \circ \varphi_p^{n-1}\} \ .$$

Diese Aussage reproduziert offensichtlich die Aussage aus Proposition 15.2 für $f = \mathrm{id}$ und der Beweis funktioniert ebenso:

Proof. Wir stellen fest, dass die Elemente $f, f \circ \varphi_p, f \circ \varphi_p^2, ..., f \circ \varphi_p^{n-1}$ verschiedene Homomorphismen definieren, denn falls

$$f\varphi_p^k = f\varphi_p^{k'}$$

gilt folgt, dass für jedes $x \in \mathbb{F}_q$ gilt

$$f(x^{p^k}) = f(x^{p^{k'}})$$

also wegen der Injektivität von f auch $x^{p^k} = x^{p^{k'}}$. Also $k = k' \mod n$. Es folgt dann aber aus Satz 11.6 wieder Gleichheit. □

Auf die Art und Weise verstehen wir nicht nur alle endlichen Körper, sondern auch alle Abbildungen dazwischen auf sehr explizite Art und Weise. Wir werden dies nun auf systematische Art und Weise formulieren mittels des Begriffes einer Kategorie.

16 Kategorien

Wir haben alle endlichen Körper bis auf Isomorphie verstanden und alle Morphismen zwischen endlichen Körpern. Um das ergebnis etwas systematischer auszudrücken wollen wir nun den Begriff einer Kategorie einführen. Eine Kategorie formalisiert im Wesentlichen den Begriff von Objekten und Morphismen den wir in der Mathematik schon oft gesehen haben: Vektrorräume und lineare Abbildungen, Körper und Körperhomomorphismen, Gruppen und Gruppenhomomorphismen etc.

Bemerkung 16.1. Wir müssen im Folgenden mit Objekten wie der "Menge aller Mengen" arbeiten. Dieser Begriff ist problematisch, vielleicht kennen sie die Russellsche Antinomie, die auf Widerpsrüchen führt. Um diese zu vermeiden benutzen wir ein etwas mächtigeres Axiomemsystem als ZFC: wir nehmen an, dass es Mengen gibt und "große Mengen" (aka Klassen). Jede Menge ist eine große Menge, aber nicht umgekehrt. Die Menge aller Mengen ist dann eine große Menge und es gibt keine Widerpsrüche. Formal betrachtet benutzen wir zwei ineinander enthaltene Modelle von ZFC. Manchmal werden auch etwas andere Axiomatisierungen verwendet (isnbesondere wenn man von Klassen spricht), aber das spielt erstmal keine Rolle solange das Auswahlaxiom auch für große Mengen gilt.

Definition 16.2. *Eine Kategorie $\mathcal{C}$ besteht aus*

- *einer großen Menge von Objekten $X, Y, Z, ...$;*
- *Für jedes Paar von Objekten X, Y einer Menge $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ von Morphismen. Wir schreiben $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ auch als $f : X \to Y$;*
- *Für je drei Objekte X, Y, Z eine Kompositionsabbildung:*

  $\circ : \mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z) \qquad (f, g) \mapsto f \circ g \qquad$ *(oder nur fg)*

sodass folgende Axiome erfüllt sind:

1. *die Komposition ist assoziativ, d.h für* $f : X \to Y$, $g : Y \to Z$ *und* $h : Z \to A$ *gilt* $h \circ (g \circ f) = (h \circ g) \circ f$.

2. *für jedes Objekt* X *existiert ein Morphismus* $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ *sodass für jeden Morphism* $f : X \to Y$ *und* $g : Z \to X$ *gilt*

$$f \circ \mathrm{id}_X = f \qquad \mathrm{id}_X \circ g = g.$$

Beispiel 16.3. 1. Wir haben die Kategorie Set aller Mengen. Die Objekte sind Mengen, Morphismen sind Abbildungen, d.h.

$$\mathrm{Hom}_{\mathrm{Set}}(X, Y)$$

ist die Menge aller Abbildung von der Menge X in die Menge Y. Die Kompositionsabbildung ist die Komposition von Abbildungen. Die Axiome sind natürlich erfüllt (die Identität ist die Identitätsabbildung).

2. Wir fixieren einen Köper K. Wir haben die Kategorie Vect_K aller Vektoräume. Die Objekte sind K-Vektoräume. Morphismen sind K-linear Abbildungen, d.h.

$$\mathrm{Hom}_{\mathrm{Vect}_K}(V, W)$$

ist die Menge aller K-linearen Abbildungen von V nach W. Die Kompositionsabbildung ist die Komposition von Abbildungen (diese ist wieder linear) und die Identität ist die Identität (diese ist linear).

3. Die Kategorie aller Körper Field.

4. Die Kategorie aller endlichen Körper Field.

5. Allgemein kann man in einer Kategorie $\mathcal{C}$ eine Teilmenge aller Morphismen auswählen und eine Kategorie $\mathcal{C}_0$ betrachten deren Objekte in dieser Teilmenge liegen. Morphismen und Komposition definiert man wie in $\mathcal{C}$. Wir sprechen dann von einer vollen Unterrkategorie (und schreiben manchmal $\mathcal{C}_0 \subseteq \mathcal{C}$).

6. point, BG

7. Präordnung (Reflexiv, transitiv)

8. Opposite $\mathcal{C}^{\mathrm{op}}$.

Die Identität id_X ist eindeutig festgelegt (wie das neutrale Element in einer Gruppe), denn falls id_X und id'_X beide die definierende Eigenschaft einer Identität erfüllen gilt

$$\mathrm{id}_X = \mathrm{id}_X \circ \mathrm{id}'_X = \mathrm{id}'_X \ .$$

Insbesondere können wir die Notation id_X eindeutig verwenden. Wir schreiben falls X ein Objekt der Kategorie $\mathcal{C}$ ist auch oft $X \in \mathcal{C}$.

Einer der Hauptphilosophien der Kategorientheorie ist es, niemals Objekte bis auf Gleichheit zu untersuchen: es macht wenig Sinn zu fragen ob zwei abstrakte Vektorräume "gleich" sind, man kann aber fragen ob sie "isomorph" sind. Den Begriff kann man in jeder Kategorie einführen:

Definition 16.4. *Isomorphismus, Objekte isomorph. (Endomorphismus, Automorphismus.)*

Beispiel 16.5.

1. Der Begriff Isomrophismus reduziert sich auf alle gleichhgenannten Begriffe die wir vorher benutzt haben: zwei Mengen sind isomorph in Set, wenn sie die gleiche Mächtigkeit haben. Es gibt dann aber natürlich viele Isomorphismen. Zwei Vektorräume sind Isomorph, wenn sie die gleiche Dimension haben etc.

2. Im Allgmeinen kann es natürlich sein, dass wir Objekte in verschiedenen Kategorien betrachten können. Zum Beispiel kann man fragen ob zwei Körper K und K' der Charakteristik 0 isomorph sind als Mengen (das ist zum Beispiel der Fall, wenn sie beide endlich über $\mathbb{Q}$ sind). Dann kann man fragen ob sie isomorph als Objekt in $\mathrm{Vect}_{\mathbb{Q}}$ sind: das ist der Fall, wenn sie die gleiche Dimension über $\mathbb{Q}$ haben. Schließlich kann man fragen, ob sie isomorph als Körper sind. Keiner der Begriffe impliziert den nächsten (es ist eine gute Übung für ihr Verständnis der bisherigen Vorlesung wenn sie sich Gegenbeispiele überlegen!). Die Kategorie ist also eigentlich zwingend notwendig, wenn man von Isomorphie spricht, wird aber oft implizit gelassen.

3. Es ist auch ein Satz, dass eine Bijektive lineare Abbildung ein Isomorphismus in Vektorräumen ist

4. Für jede Kategorie $\mathcal{C}$ und $X \in \mathcal{C}$ bilden die Automorphismen eine Gruppe $\mathrm{Aut}_{\mathcal{C}}(X)$ mittels Komposition von Abbildungen.

5. Wenn $f : X \to Y$ ein Isomorphismus ist, dann ist das Inverse eindeutig bestimmt, d.h. zwei Inverse g und g' sind gleich, denn es gilt

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ g') = (g \circ g) \circ g' = \mathrm{id}_X \circ g' = g' \ .$$

Definition 16.6. *Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ ist eine Zuordnung, die jedem Objekt $X \in \mathcal{C}$ ein Objet $F(X) \in \mathcal{D}$ zuordnet (also eine Abbildung auf den Objektmengen) und für jeden Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ einen Morphismus $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ sodass gilt*

$$F(f \circ g) = F(f) \circ F(g) \qquad F(\mathrm{id}_X) = \mathrm{id}_{F(X)} \ .$$

Beispiel 16.7.

1. Vergissfunktoren $\mathrm{Vect}_K \to \mathrm{Set}$ und $\mathrm{Field} \to \mathrm{Vect}_K$

2. Die Inklusion einer vollen Unterkategorie

3. Ein Funktor $\mathrm{pt} \to \mathcal{C}$ ist genau ein Objekt in $\mathcal{C}$, denn die Identität muss auf die Identität gehen.

4. Ein Funktor $BG \to \mathcal{C}$ ist gegeben durch ein Objekt $X \in \mathcal{C}$ zusammen mit einem Gruppenhomomorphismus $G \to \mathrm{Aut}_{\mathcal{C}}(X)$. Das ist das gleiche wie eine (links)-Wirkung von G auf X.

5. Sei I eine Prägeordnete Menge. Dann ist ein Funktor $(I, \leq) \to \mathcal{C}$ gegebnen durch die folgenden Daten: für jedes $i \in X$ ein Objekt C_i und für jedes Paar (i, j) mit $i \leq j$ ein Morphismus $C_i \to C_j$ sodass gilt: ....Komposition, Idenität. Falls I gerichtet ist und $\mathcal{C} =$ Field, dann ist das genau das gleiche wie eine I-indiziertes Diagram vom Körpern (wie vorher eingeführt, siehe Definition 12.4).

6. Ein Funktor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ ist konkret das folgende: eine Zuordnung $X \in \mathcal{C} \mapsto F(X) \in \mathcal{D}$. Für jeden Morphismus $f : X \to Y$ in $\mathcal{C}$ einen Morphismus $F(f) : F(Y) \to F(X)$ in $\mathcal{D}$, sodass gilt ....

   Ein Funktor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ wird auch kontravarianter Funktor von $\mathcal{C}$ nach $\mathcal{D}$ genannt (und ein Funktor $\mathcal{C} \to \mathcal{D}$ dann kovarianter Funktor). Dies ist das gleiche Datum wie ein Funktor $\mathcal{C} \to \mathcal{D}^{\mathrm{op}}$.

7. Wir haben den Funktor $\mathrm{Vect}_K^{\mathrm{op}} \to \mathrm{Vect}_K$ der einem K-Vektorraum V den dualraum V^* und jeder K-linearen Abbildung $f : V \to W$ die duale Abbildung $f^* : W^* \to V^*$ zuordnet.

8. Es gibt für jede Gruppe G den Funktor $BG^{\mathrm{op}} \to BG$ gegeben durch $g \mapsto g^{-1}$.

17 Limits und natürliche Äquivalenzen

Definition 17.1. *1. Seien I und $\mathcal{C}$ Kategorien und $F : I \to \mathcal{C}$ ein Funktor. Ein Kegel über F ist ein Objekt $X \in \mathcal{C}$ zusammen mit Morphismen $p_i : X \to F(i)$ für jedes $i \in I$ sodass für jeden Morphismus $f : i \to j$ in I das Diagram*

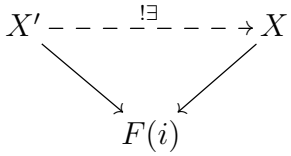
$$\begin{array}{ccc} X & & \\ \downarrow{\scriptstyle p_i} & \searrow^{p_j} & \\ F(i) & \xrightarrow{F(f)} & F(j) \end{array}$$

kommutiert.

2. Analog ist ein Kegel unter F (auch als Ko-Kegel bezeichnet) ein Objekt $X \in \mathcal{C}$ zusammen mit Morphismen $\iota_i : F(i) \to X$ sodass die analogen Diagramme kommutieren:

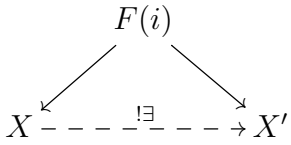
$$\begin{array}{ccc} F(i) & \xrightarrow{F(f)} & F(j) \\ & \searrow^{\iota_i} & \downarrow{\scriptstyle \iota_j} \\ & & X \end{array}$$

3. *Ein Kegel über F der Form (X, p_i) heisst Limes des Diagramms F, falls für jeden weitern Kegel über F der Form (X', p_i') genau eine Abbildung $X' \to X$ existiert sodass alle Diagramme*



kommutieren. Wir schreiben dann auch $X = \lim_I F$.

4. *Ein Kegel über F der Form (X, ι_i) heisst Kolimes des Diagramms F, falls für jeden weitern Kegel unter F der Form (X', ι_i') genau eine Abbildung $X \to X'$ existiert sodass alle Diagramme*



kommutieren. Wir schreiben dann auch $X = \lim_I F$.

Satz 17.2. *Für ein gegebenes Diagram $I \to \mathcal{C}$ sind Kolimes und Limes, falls sie existieren, eindeutig bis auf eindeutige Isomorphie.*

Beispiel 17.3. Sei $I = \emptyset$ die leere Kategorie. Dann gibt es genau einen Funktor $I \to \mathcal{C}$. Ein Kegel über oder unter diesem Funktor ist dann einfach ein Objekt $X \in \mathcal{C}$. Dieses ist der Kolimes falls es folgende universelle Eigenschaft hat: für jedes weitere Objekt $X' \in \mathcal{C}$ existiert genau ein Morphismus $X \to X'$. In diesem Fall nennen wir X auch das *initiale Objekt* von $\mathcal{C}$. Dual ist X der Limes, wenn fúr jedes X' genau ein Morphismus $X' \to X$ existiert. Dann heisst X das terminale Objekt von $\mathcal{C}$.
Als Beispiel sei $\mathcal{C} = \mathrm{Set}$. Dann ist die leere Menge initial und die einelementige Menge $\mathrm{pt} \in \mathrm{Set}$ terminal.
Als weiteres Beispiel sei $\mathcal{C} = \mathrm{Vect}_k$, Dann ist der 0-Vekotrraum sowohl initial als auch terminal.
Schließlich betrachte die Kategorie Field. Diese hat kein initilales und kein terminales Objekt. Denn für jeden Körper K gibt es einen Körper K' sodass kein Morphismus $K \to K'$ und kein Morphismus $K' \to K$ existieren. Dazu nimmt man einfach K' mit anderer Charakteristik als K.

Beispiel 17.4. Sie I die einer gerichtet Menge I zugeordnete Kategorie. Dann reduziert sich das Konzept eines Kolimits von $F : I \to \mathcal{C}$ für $\mathcal{C} = \mathrm{Field}$ auf das Konzept des gerichteten Kolimits von Körpern das wir vorher diskutiert haben.

Beispiel 17.5. Sie S eine Menge. Wir betrachten eine Kategorie S^δ welche die Elemente aus S als Objekte hat und sodass

$$\mathrm{Hom}_{S^\delta}(s,t) = \begin{cases} \{\mathrm{id}\} & \text{falls } s = t \\ \emptyset & \text{sonst} \end{cases}$$

Dies wir auch die diskrete Kategorie auf S genannt. Ein Funktor $S^\delta \to \mathcal{C}$ ist das gleiche wie eine Familie $(X_s)_{s\in S}$ von Objekten in $\mathcal{C}$. Ein Kolimes besteht aus einem Objekt $X \in \mathcal{C}$ zusammen mit Morphismen $X_s \to X$ für alle s sodass für jede Familie von Morphismen $f_s : X_s \to Y$ genau ein Morphismus $X \to Y$ existiert der mit den Abbildungen von X_s kommutiert. Wir nennen dies auch ein Koprodukt.
Analog besteht ein Limes aus einem Objekt X mit Abbildungen $X \to X_s$ sodass für jede weiter Familie von Abbildunge $Y \to X_s$ genau ein Morhpismus $Y \to X$ existiert, der mit den Abbbildungen nach X_s kommutiert. Wir nennen einen solchen Limes aus Produkt.
Als Beispiel betrachten wir $\mathcal{C} = \text{Set}$. Dann ist $\coprod X_s$ ein Koprodukt der Familie X_s. Analog ist $\prod X_s$ ein Produkt.
In der Kategorie Vect_K ist $\oplus X_s$ ein Koprodukt der Familie X_s und $\prod X_s$ ein Produkt. Insbesondere stimmen für endliches S Korprodukt und Produkt überein.

Es gibt ein paar elementare Eigenschaften von Funktoren: Funktoren senden Isomorphismen auf Isomorhismen. Man kann Funktoren komponieren: gegeben $F : \mathcal{C} \to \mathcal{D}$ und $G : \mathcal{D} \to \mathcal{E}$ so kann man die Komposition $G \circ F : \mathcal{C} \to \mathcal{E}$ in der (hoffentlich) offensichtlichen Art und Weise definieren. Zum Beispiel ist der Vegissfunktor $\text{Field}_K \to \text{Set}$ die Komposition der beiden Vergissfunktoren $\text{Field}_K \to \text{Vect}_K \to \text{Set}$ Ausserdem gibt es auf jeder Kategorie $\mathcal{C}$ den Identitätsfunktor $\text{id}_\mathcal{C} : \mathcal{C} \to \mathcal{C}$. Man könnte also so etwas wie die Kategorie der Kategorien betrachten. Das wollen wir aber nicht tun, denn zunächst wollen wir verschiedene Funktoren $F, G : \mathcal{C} \to \mathcal{D}$ miteinander vergleichen. Zum Beispiel, wenn $\mathcal{C} = \text{pt}$ so hat man einfach zwei verschiedene Objekte in $\mathcal{D}$ und um diese zu vergleichen betrachten wir Morphismen dazwischen. Das wird vom folgenden Begriff verallgemeinert:

Definition 17.6. *Gegeben zwei Funktoren $F, G : \mathcal{C} \to \mathcal{D}$ dann ist eine Natürliche Transformation η eine Zuordnung jedem Objekt $X \in \mathcal{C}$ einen Morphistmus $\eta_X : F(X) \to G(X)$ zuordnet, sodass für jeden Morphismus $f : X \to Y$ in $\mathcal{C}$ gitl, dass das Diagram*

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ \downarrow{\scriptstyle \eta_X} & & \downarrow{\scriptstyle \eta_Y} \\ G(X) & \xrightarrow{G(f)} & G(Y) \end{array}$$

Wir sagen auch, die Abbildungen $\eta_X F(X) \to G(X)$ sind natürlich in X.

Beispiel 17.7.

1. Auf jedem Funktor $F : \mathcal{C} \to \mathcal{D}$ gibt es die Identitätstransformation.

2. Sei $()^{**} : \text{Vect}_k \to \text{Vect}_k$ der doppel-dual Funktor, der jedem Vektorraum sein doppelten Dualraum zuordnet (also die Komposition des dualen Funktors mit sich selbst). Dann ist die kanonische Abbildung $V \to V^{**}$ für jeden Vektorraum natürlich in V, d.h. sie bildet eine natürliche Transformation vom Identitätsrunktor zum Funktor $(-)^{**}$.. Um das zu sehen

müssen wir zeigen, dass für jede lineare Abbildung $V \to W$ das Diagram

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow & & \downarrow \\ V^{**} & \xrightarrow{f^{**}} & W^{**} \end{array}$$

kommutiert. Das sieht man einfach indem man sich überlegt das beide Kompositionen ein $v \in V$ auf die Abbildung $W^* \to K$ schicken die φ auf $\varphi(f(v))$ sendet.

3. Angenommen wir haben Funktoren $F, G, H : \mathcal{C} \to \mathcal{D}$ und natürliche Transofmrationen $\eta : F \to G$ sowieo $\epsilon : G \to H$. Dann können wir eine Komposition $\epsilon \circ \eta$ definieren durch $(\epsilon \circ \eta)_X = \epsilon_X \circ \eta_X$. Dies ist offensichtlich wieder eine natürliche Transformation.

4. Gegeben eine natürlich Transformation $\eta : F \to G$ von Funktoren $F, G : \mathcal{C} \to \mathcal{D}$ und ein Funktor $H : \mathcal{D} \to \mathcal{E}$. Dann haben wir eine natürliche Transforrmation $H \circ \eta : HF \to HG$ wie folgt: wir wenden H an auf $\eta_x : FX \to GX$.

5. Analog zum letzten Beispiel haben wir für $\eta : F \to G$ und $E : \mathcal{B} \to \mathcal{C}$ eine natürliche Transformation $\eta E : FE \to GE$ definiert wie folgt: Wir setzen $(\eta E)_B := \eta_{E(B)}$.

Definition 17.8. *Wir formen die Funktorkategorie* $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ *deren Objekte Funktoren* $\mathcal{C} \to \mathcal{D}$ *sind und deren Morphismen natürliche Transformationen. Komposition ist die Komposition von natürlichen Transformationen. Wir schrieben diese Kategorie auch als* $\mathcal{D}^{\mathcal{C}}$.

Bemerkung 17.9. Im Allgemeinen sind die Morphismen-Mengen in $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ selbst große Mengen, aber wir ignorieren diese Mengentheoretische Subtilität hier.

Beispiel 17.10. 1. Es gilt $\mathrm{Fun}(\mathrm{pt}, \mathcal{C}) = \mathcal{C}$.

2. Die Kategorie $\mathrm{Fun}(BG, \mathrm{Set}) = \mathrm{Set}^{BG}$ hat als Objekte Mengen mit einer G-Wirkung, i.e. eine Menge X zusammen mit einem Gruppenhomomorphismu

$$G \to \mathrm{Aut}(X) \qquad g \mapsto l_g \ .$$

Äquivalent beschreiben wir dies als Abbildung

$$G \times X \to X \qquad (g, x) \mapsto g \cdot x = l_g(x)$$

sodass gilt $(gh) \cdot x = g \cdot (h \cdot x)$ und $1 \cdot x = x$. Wir sprechen auch von einer Linkswirkung von G auf X. Ein Morphismus in $\mathrm{Fun}(BG, \mathrm{Set})$ zwischen X und Y besteht aus einer Abbildung $f : X \to Y$ sodass für jedes $g \in G$ und $x \in X$ gilt $f(gx) = gf(x)$. Wir nennen solche Abbildungen auch G-äquivariant.

3. Ähnlich kann man Field^{BG} betrachten oder $(\mathrm{Field}_{K/})^{BG}$. Diese besteht aus Körpern mit einer Wirkung von G durch Körperautomorhismen bzw. Morphismen unter K.

Lemma 17.11. *Eine natürliche Transformation η ist genau dann ein Isomorphismus in der Funktorkategorie, wenn gilt: für jedes $X \in \mathcal{C}$ ist $\eta_X : F(X) \to G(X)$ ein Isomorphismus in $\mathcal{C}$. In diesem Fall nennen wir η einen natürlichen Isomorphismus.*

Proof. Eine Richtung ist trivial. Für die andere sei η eine natürliche Trafo die punktweise ein iso ist. Dann bilden wir eine neue Transformation

$$\mu_X := (\eta_X)^{-1}$$

und behaupten, dass diese wieder natürlich ist. Wir müssen zeigen, dass für jedes f das Diagram kommutiert... □

Im Fall von G-Mengen reduziert sich das Statement darauf, dass eine Abbildung $X \to Y$ von G-Mengen ein Isomorphismus ist, wenn die unterliegende Abbildung von Mengen eine Bijektion ist (alsio mit anderen Worten: die Inverse ist wieder äquivariant).

18 Kategorien von Gruppenwirkungen

Falls eine natürliche transformation ein Iso ist, nennen wir sie natürlichen Isomorphismus und die Funktoren natürlich isomorph.

Beispiel 18.1. Die Trafo $V \to V^{**}$ ist ein Iso von Funktoren $\mathrm{FinVect}_K \to \mathrm{FinVect}_K$.

Wir wollen nun zwei Funktoren als "gleich" betrachten, wenn sie natürlich Isomorph sind. Daraus ergibt sich dann folgender Begriff davon, wann wir Kategorien als äquivalent betrachten:

Definition 18.2. *Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heisst Äquivalenz von Kategorien, falls ein Funktor $G : \mathcal{D} \to \mathcal{C}$ existiert, sodass $G \circ F \cong \mathrm{id}_{\mathcal{C}}$ und $F \circ G \cong \mathrm{id}_{\mathcal{D}}$. Wenn eine solche Äquivalenz existiert, dann sagen wir, dass $\mathcal{C}$ und $\mathcal{D}$ äquivalent sind und schreiben $\mathcal{C} \simeq \mathcal{D}$. Der Funktor G heisst das Inverse von F.*

Natürlich ist dies eine Äquivalenzrelation auf Kategorien.

Beispiel 18.3. Die Kategorie $\mathrm{FinVect}_K$ ist äquivalent zu ihrer opponierten $\mathrm{FinVect}_K^{\mathrm{op}}$ mittels des Funktors $\mathrm{FinVect}_K \to \mathrm{FinVect}_K^{\mathrm{op}}$ gegeben durch $V \mapsto V^*$. Der Inverse ist der 'gleiche' Funktor und die beiden trafos sind die vorher diskutierten (wir benutzen hier, dass ein Funktor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}^{\mathrm{op}}$ das gleiche ist wie ein Funktor $\mathcal{C} \to \mathcal{D}$).

Satz 18.4. *1. Eine Äquivalenz von Kategorien $\mathcal{C} \to \mathcal{D}$ ist volltreu, das heisst für je zwei Objekte $X, Y \in \mathcal{C}$ gilt, dass die induzierte Abbildung*

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(FX, FY)$$

eine Bijektion ist.

2. *Eine Äquivalenz $\mathcal{C} \to \mathcal{D}$ ist essentiell surjektiv, d.h. für jedes $d \in \mathcal{D}$ existiert ein $c \in \mathcal{C}$ sodass $F(c)$ isomorph zu d ist.*

3. *Es gilt auch die Umkehrung: jeder volltreue und essentiell surjektive Funktor ist eine Äquivalenz.*

Proof. Übung. □

Beispiel 18.5. Betrachte die Kategorie der endlich-dimensionalen Vektoräume $\mathrm{FinVect}_K$ und die volle Unterkategorie $\mathrm{FinVect}_K^{std} \subseteq \mathrm{FinVect}_K$ mit Objekten K^n. Dann ist die Inklusion eine Äquivalenz von Kategorien. So manche Vorlesung lineare Algebra spielt sich in der ersten Kategorie ab.

Beispiel 18.6. Betrachte die voll Unterkategorie von $\mathrm{Field}^{alg}_{/\mathbb{R}} \subseteq \mathrm{Field}_{\mathbb{R}/}$ bestehend aus den algebraisch abgeschlossenen Körpern. Wir haben einen Funktor $BC_2 \to \mathrm{Field}^{alg}_{/\mathbb{R}}$ welcher durch die komplexen Zahlen mit dem $\mathbb{R}$-linearen Automorphismus komplexe Konjugation gegeben ist. Dieser Funktor ist eine Äquivalenz von Kategorien.

Beispiel 18.7. Betrachte allgmeiner für einen beliebigen Körper K die Kategorie $\mathrm{Field}^{alg}_{K/} \subseteq \mathrm{Field}_{K/}$. Wir wählen einen algebraischen Abschluss $\overline{K}$ und betrachten die Gruppe $G := \mathrm{Aut}_K(\overline{K})$. Wir bekommen einen Funktor $BG \to \mathrm{Field}^{alg}_{K/}$ und dieser ist eine Äquivalenz von Kategorien.

Die letzten Beispiele lassen sich alle auf die folgende Art verallgemeinern: gegeben ein Kategorie $\mathcal{C}$ und eine Menge von Objekten sodass aus jeder Isomorphieklasse mindestens ein Element enthalten ist. Dann ist die volle Unterkategrorie auf $\mathcal{C}_0$ äquivalent zu $\mathcal{C}$.

Gegeben sei nun eine Gruppe G die auf einer Menge X operiert oder äquivalent ein Funktor $BG \to \mathrm{Set}$.

Definition 18.8. *Wir definieren eine Äquivalenzrelation auf X durch*

$$x \sim y :\Leftrightarrow \exists g : y = gx$$

Man sieht leicht, dass dies in der Tat eine Äquivalenzrelation ist. Wir definieren den Quotienten X/G als die Menge der Äquivalenzklassen. Eine Äquivalenzklasse

$$[x] = Gx \subseteq X$$

wird als Orbit (von x) bezeichnet.

Beispiel 18.9. Für eine Untergruppe $H \subseteq G$ ist $X := G/H$ eine G-Menge mit der Linksmultiplikation von G:

$$g \cdot [g'] = g \cdot g'H := [gg'] = gg'H$$

In diesem Fall besteht der Quotient aus einem einzigen Punkt.

Warnung 18.10. *Sei H eine Untergruppe von G. Dann operiert H durch Linksmultiplikation auf G, aber der Quotient G/H den wir vorher definiert (für Gruppen) haben stimmt aus Konventionsgründen nicht ganz mit G/H (wir hätten Rechntsnebenklassen verwenden müssten). Wir können H aber durch*

$$h \cdot g := gh^{-1}$$

operieren lassen, dann stimmt der Quotient mit G/H überein.

Proposition 18.11. *Die Menge X/G zusammen mit der Projektionsabbildung $X \to X/G$ ist der colimes des Diagrams $BG \to$ Set.*

Proof. Ein Kegel unter diesem Funktor besteht aus einer Menge Y zusammen mit einer Abbildung $p : X \to Y$ sodass für jedes $g \in G$ gilt, dass $p(gx) = p(x)$. Eine solche Abbildung faktorisiert aber eindeutig über die Äquivalenzrelation. □

Definition 18.12. *Für $x \in X$ ist die Isotropiegruppe von x gegeben durch*

$$G_x := \{g \in G \mid gx = x\} .$$

Sie ist eine Untergruppe von G.

Proposition 18.13. *Für jede G-Menge X ist die Abbildung*

$$G/G_x \to Gx \qquad [g] \mapsto gx$$

eine wohldefinierte Bijektion. Sie ist außerdem G-equivariant für die Linksmultiplikation von G auf beiden Seiten.

Proof. Die Abbildung $G \to Gx$ die g auf gx sendet, schickt g und g' genau dann auf das gleiche Element, wenn gilt $gx = g'x$, also $g^{-1}g' \in G_x$. Das bedeutet aber, dass $[g] = [g']$ in G/G_x. Das zeigt, dass die Abbildung wohldefiniert und Injektiv ist. Surjektivität ist klar. Äquivarianz auch. □

Korollar 18.14. *Für eine endliche Gruppe G gilt $|G| = |G_x| \cdot |Gx|$. Insbesondere teilt die Kardinalität jedes Orbits die Kardinalität der Gruppe.*

Definition 18.15. *Für eine G-Wirkung auf X definieren wir die Fixpunkte als*

$$X^G := \{x \in X \mid gx = x \forall g \in G\} .$$

Die folgenden Bedingungen sind offensichtlich äquivalent für $x \in X$:

1. $x \in X^G$.

2. $G_x = G$

3. $Gx = \{x\}$

Proposition 18.16. *X^G zusammen mit der Abbildung $X^G \to X$ ist der Limes des Diagramms $BG \to$ Set.*

Wir können analog auch Körper K mit einer G-Wirkung durch Körperhomomorphismen betrachten. Dann ist K^G offensichtlich selbst ein Körper und es ist der Limes des entsprechenden Diagramms in Field (Warnung: K/G ist kein Körper und es gibt im Allgmeinen keinen Kolimes des entsprechenden Diagramms in der Kategorie Field).

Definition 18.17. *Für eine Primzahl p heisst eine endliche Gruppe deren Ordnung eine Potenz p^r von p ist eine p-Gruppe.*

Proposition 18.18. *Sei G eine endliche p-Gruppe und G operiere auf einer endlichen Menge X. Dann gilt*

$$|X| = |X^G| \mod p$$

Proof. X zerlegt sich in Orbits mit einem Element (die Fixpunkte) und Orbits der Form G/G_x für G_x eine echte Untergruppe von G. Diese hat damit Ordnung p^m mit $m < r$ und daher ist die Ordnung von G/G_x durch p teilbar und das Resultat folgt. □

Insbesondere hat jede Wirkung von G auf einer Menge X deren Ordnung nicht durch p teilbar ist ein Fixpunkt.

Beispiel 18.19. Betrachte die Wirkung von G auf sich selbst durch Konjugation, d.h.

$$(g, x) \mapsto gxg{-}1$$

Dies ist offensichtlich eine Wirkung. Der Quotient heisst auch die Menge der Konjugationsklassen und die Stabilisatoruntergruppe von $x \in G$ ist gegeben durch

$$\{g \in G \mid gxg^{-1} = x\}$$

und heisst der Zentralisator von x. Die Fixpunkte sind die $x \in G$ sodass $gxg^{-1} = x$ für alle g, also das Zentrum $Z(G)$.

Korollar 18.20. *Eine endliche, nicht-triviale p-Gruppe G hat nicht-triviales Zentrum.*

Proof. Weil $Z(G)$ die Fixpunkte sind gilt modulo p:

$$|Z(G)| = |G| = 0$$

Also kann nicht $Z(G) = \{1\}$ sein. □

Satz 18.21 (Struktursatz für p-Gruppen)**.** *Für jede endliche p-Gruppe G existiert eine Folge von normalen Untergruppen*

$$\{e\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

sodass $G_{i+1}/G_i \cong \mathbb{Z}/p$ (dies ist ein Isomorphismus von Gruppen, denn G_i ist auch normal in G_{i+1}).

Proof. Wir verwenden Induktion über die Anzahl der Elemente von G. Für G trivial ist die Aussage klar. Anderenfalls nehmen wir an, dass G nicht-trivial ist und wir die Aussage bereits für alle p-Gruppen kleinerer Ordnung gezeigt haben. Weil G nicht-trivial ist hat hst G ein nicht-triviales Zentrum $Z(G)$ von Ordnung p^m. Wir finden also nach dem Satz von Lagrange ein Element $x \in Z(G)$ der Ordnung p (durch Übergang zu einem Potenz eines Elementes der Ordnung p^k). Dann setzen wir

$$G_1 := \langle x \rangle$$

Diese Untergruppe ist als Untergruppe des Zentrums normal in G und isomorph zu $\mathbb{Z}/p$. Jetzt betrachten wir die p-Gruppe $G' := G/G_1$. Diese hat kleinere Ordnung. Daher existiert für diese Gruppe bereits eine Filtration der gewünschten Art:

$$\{e\} = G'_0 \subseteq G'_1 \subseteq G'_2 \subseteq ... \subseteq G_{n-1} = G$$

Wir setzen nun $G_i := \pi^{-1}(G_{i-1})$ für $\pi : G \to G/G_1$. Diese Untergruppen sind normal (Urbilder von normalen Untergruppen) und die Quotienten sind gegeben durch $\mathbb{Z}/p$. □

19 Die Kategorie der endlichen Körper

Definition 19.1. *Eine Gruppenwirkung von G auf einer Menge X heisst frei, falls $gx = g$ für beliebige x und g bereits impliziert, dass $g = 1$, oder äquivalent dass die Abbildung $G \to \mathrm{Aut}_{\mathrm{Set}}(X)$ injektiv ist.*
Sie heisst treu, falls $gx = x$ für alle x impliziert, dass $g = 1$.
Sie heisst transitiv, wenn $X/G = \mathrm{pt}$ oder äquivalent $X = Gx$ für jedes $x \in X$.

Beispiel 19.2. Offensichtlich ist jede freie Wirkung auch treu. Das Gegenteil gilt nicht, zum Beispiel wirkt Σ_n treu auf der Menge mit n-Elementen, aber für $n \geq 3$ nicht frei (so lässt das Element $(12) \in \Sigma_3$ das Element $3 \in \{1, 2, 3\}$ fest).

Für eine freie G-Menge X ist jeder Orbit in Bijektion zu G selbst (mit Linkswirkung von G). Also ist jede freie G-Menge X die disjunkte Vereinung ihrere Orbits, also von der Form

$$X = \coprod_{i \in I} Gx_i \cong G \times I$$

für I eine Menge ($I \cong X/G$) wobei G auf dem linken Faktor wirkt. Für jede transitive G-Menge X ist die Abbildung

$$G/G_x \to X$$

ein Isomorphismus von G-Mengen (wobei G auf G/G_x von Links operiert). Insbesondere sind solche bis auf Isomorphe stets von der Form G/H für H eine Untergruppe von G. Eine freie und transitive G-Menge X ist insbesondere isomorph zu G mit linkswirkung von G (und ein solcher Isomorphismus hängt von der Wahl eines Punktes in X ab).

Beispiel 19.3. Betrachte die volle Unterkategorie von Set^{BG} auf den freien und transitiven G-Mengen. Es gibt einen Funktor von BG in diese Kategorie, welcher den Punkt auf G schickt (als G-Menge mit linksmultiplikation) und dieser ist eine Äquivalenz von Kategorien.

Lemma 19.4. *1. Jeder G-äquivarianten Homomorphismus $X \to X'$ zwischen transitiven G-Mengen ist surjektiv.*

2. Für die zwei G-Mengen G/H und G/H' sind G-äquivairante Abbildungen gegeben durch

$$\mathrm{Hom}_{\mathrm{Set}^{BG}}(G/H, G/H') \cong \{[g] \in G/H' \mid gHg^{-1} \subseteq H'\} \qquad f \mapsto f([1]) \ .$$

3. Insbesondere sind G/H und G/H' genau dann isomorph als G-Mengen, wenn H und H' konjugiert sind, d.h. wenn es ein $g \in G$ gibt sodass $gHg^{-1} = H'$.

Proof. Sei $f : X \to X'$ surjektiv und $x \in X$. Dann ist $f(x)$ im Bild. Jedes weitere Element in X' ist von der Form $gf(x) = f(gx)$ also auch im Bild.
Sei $f : G/H \to G/H'$ äquivariant. Dann gilt

$$f([g]) = f(g \cdot [1]) = gf([1])$$

also ist f eindeutig durch $f([1])$ bestimmt. Ausserdem gilt, dass für jedes $h \in H$ dass

$$h \cdot f(1) = f(h) = f(1)$$

in G/H', also $f(1)h^{-1}f(1)^{-1} \in H'$. Umgekehrt ist es einfach zu sehen, dass die letzte Bedingung auch eine wohldefinierte Abbildung definiert.

□

Es folgt, dass Isomorphieklassen von Transitiven G-Mengen in bijektion zu Konjugationsklassen von Untergruppen von G stehen.

Beispiel 19.5. Sei $G = \mathbb{Z}$. Eine $\mathbb{Z}$-Menge ist eine Menge X mit einer Bijektion $X \to X$. Die transitiven $\mathbb{Z}$-Mengen sind bis auf Isomorphie alle von der Form $\mathbb{Z}/n$ oder $\mathbb{Z}$ wobei die Bijektion durch Addition von 1 gegeben ist. Einen Isomorphismus zu einer der Standard Menge $\mathbb{Z}$ oder $\mathbb{Z}/n$ zu wählen ist

äquivalent dazu ein Element aus X zu wählen. Jeder Endomorphismus einer endlichen transitiven $\mathbb{Z}$-Menge ist ein Automorphismus und es gilt

$$\mathrm{Aut}_{\mathrm{Set}^{B\mathbb{Z}}}(\mathbb{Z}/n) = \mathbb{Z}/n$$

Darüberhinaus gilt

$$\mathrm{Hom}_{\mathrm{Set}^{B\mathbb{Z}}}(\mathbb{Z}/n, \mathbb{Z}/m) = \begin{cases} \emptyset & \text{falls } m \text{ nicht } n \text{ teilt} \\ \mathbb{Z}/m & \text{sonst} \end{cases}$$

Wir stellen fest, dass diese Kategorie aussieht wie die opponierte von der Kategorie $\mathrm{FinField}_{\mathbb{F}_p}$ von endlichen Körpern der Charakteristik p.

Satz 19.6. *Es existiert eine Äquivalenz von Kategorien zwischen* $(\mathrm{FinField}_{\mathbb{F}_p})^{\mathrm{op}}$ *und der Kategorie der endlichen, transitiven $\mathbb{Z}$-Mengen. Eine solche Äquivalenz hängt von der Wahl eines algebraischen Abschlusses $\overline{\mathbb{F}}_p$ ab.*

Proof. Wir betrachten den Funktor

$$(\mathrm{FinField}_{\mathbb{F}_p})^{\mathrm{op}} \to \mathrm{Set}^{B\mathbb{Z}} \qquad K \mapsto \mathrm{Hom}_{\mathrm{Field}}(K, \overline{\mathbb{F}}_p) \ .$$

wobei auf $\mathrm{Hom}_{\mathrm{Field}}(K, \overline{\mathbb{F}}_p)$ den Frobenius Automrophismus φ_p von K wirken lassen (oder äquivalent den von $\overline{\mathbb{F}_p}$). Jeder Morphismus von $K \to \overline{\mathbb{F}}_p$ landet in dem endlichen Körper $\mathbb{F}_{p^n}$ falls K genau p^n Elemente hat. Insbesondere ist dies durch eine transitive $\mathbb{Z}$-Menge mit n-Elementen gegeben und somit ist dieser Funktor ist essentiell surjektiv auf die entsprechende Unterkategorie (Proposition 15.2). Ausserdem ist er volltreu (Prop 15.3). □

Man kann auch den Umkehrfunktor explizit beschrieben: dieser sendet eine $\mathbb{Z}$-Menge X auf den Körper $\mathrm{Hom}_{\mathrm{Set}^{B\mathbb{Z}}}(X, \overline{\mathbb{F}}_p)$ wobei die $\mathbb{Z}$-Wirkung auf $\overline{\mathbb{F}_p}$ durch den Frobenius gegeben ist und dies als Körper mit der Komponentenweisen addition aufgefasst wird. Insbesondere für $X = \mathbb{Z}/n$ bekommen wir genau die Teilmenge $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_p$.

20 Separable Körpererweiterungen

In Kapitel 15 haben wir für die Klassifikation von endlichen Körpern benutzt, dass das Polynom $x^q - x$ nur einfache Nullstellen hat. Das wollen wir nun systematisch untersuchen.

Lemma 20.1. *Sei $K \to L$ eine Körpererweiterung und $f, g \in K[x]$. Dann gilt*

$$\mathrm{ggt}_K(f, g) = \mathrm{ggt}_L(f, g).$$

Proof. Es gilt, dass der ggT eindeutig bestimmt ist durch

$$\mathrm{ggt}_K(f, g) = af + bg$$

mit $a, b \in K[x]$ und dass er sowohl f als auch g teilt. Dasselbe gilt dann aber auch über L sodass es da auch der ggT ist. (Man könnte auch mit Idealen argumentieren...). □

Definition 20.2. *Ein Polynom $f \in K[x]$ heisst separabel, wenn es in einem algebraischen Abschluss $\overline{K}$ keine mehrfachten Nullstellen hat.*

Proposition 20.3. *Ein Polynom $f \in K[x]$ ist genau dann separabel, wenn f und f' in $K[x]$ teilerfremd sind.*

Proof. Angenommen f und f' sind teilfremd. Dann sind sie auch teilerfremd über $\overline{K}$ nach dem Lemma. Nach Proposition 10.11 hat f also über $\overline{K}$ keine mehrfachen Nullstellen.
Falls umgekehrt f keine mehrfachten Nullstellen hat, so sind f und f' über $\overline{K}$ teilerfremd (weil alle irreduziblen Teiler linear sind) und daher auch über K nach dem Lemma. □

Beispiel 20.4.

1. Das Polynom $f(x) = x^{p^n} - x$ ist separabel über jedem Körper der Charakteristik p, denn dann gilt, dass die Ableitung gleich $f'(x) = 1$ ist. Insbesondere sind endliche Körper separabel über $\mathbb{F}_p$.

2. Teiler von separablen Polynomen sind separabel, insbesondere ist jeder irreduzible Faktor von $x^{p^n} - x$ separabel.

3. Betrachte die Körpererweiterung

$$K = \mathbb{F}_p(t) \to \mathbb{F}_p(s) \qquad t \mapsto s^p \ .$$

Man kann $\mathbb{F}_p(s)$ dann auch als $\mathbb{F}_p(t^{1/p})$ schreiben. Die Erweiterung entsteht also durch adjungieren einer p-ten Wurzel zu t. Das Element s wird annihiliert von dem Polynom $x^p - t \in K[x]$ welches irreduzibel ist. Dazu stellen wir fest, dass die Körpererweiterung den Grad p hat, da eine Basis über K durch $1, s, s^2, ..., s^{p-1}$ gegeben ist (wie man sich leicht überlegt). Das Polynom ist aber nicht separabel, da die Ableitung -1 ist. Es folgt, dass das Element s nicht separabel über K ist und damit die Erweiterung auch nicht separabel ist.

Korollar 20.5. *Für ein irreduzibles Polynom f über $K[x]$ sind äquivalent:*

1. *f ist nicht separabel*
2. *$f' = 0$*
3. *Es gilt $\mathrm{char}(K) = p$ und $f(x) = g(x^p)$ für ein Polynom $g \in K[x]$*

Proof. (1) $\Rightarrow$ (2) ist klar da f irreduzibel und f' echt kleineren Grad hat. Da f nicht konstant ist, ist auch klar, dass $f' = 0$ nur dann möglich ist, wenn $\mathrm{char}(K) = p$ und f nur Koeffizienten vor den p-power Potenzen hat. □

Definition 20.6. *Sei L/K eine Körpererweiterung. Dann heisst $\alpha \in L$ separabel, wenn es Nullstelle eines Separablen Polynoms ist (äquivalent, es ist algebraisch und das Minimalpolynom ist separabel). Die Erweiterung L/K heisst separabel, wenn jedes Element separabel ist.*

Beispiel 20.7. Jede Körpererweiterung über eine Körper der Charakteristik 0 ist separabel.
Angenommen K ist ein Körper der Charakteristik p, der Perfekt ist, d.h. sodass der Frobenius ein Isomorphismus ist. Zum Beispiel jeder endliche Körper. Dann ist auch jede Körpererweiteiterung separabel, denn ein irreduzibles Polynom $f \in K[x]$ welches nicht separabel ist, wäre von der Form

$$f(x) = g(x^p) = \tilde{g}(x)^p$$

wobei für $g(x) = \sum a_i x^i$ das Polynom $\tilde{g}(x) = \sum b_i x^i$ mit $b_i^p = a_i$. Also ist f nicht irreduzibel im Widerpspruch zur Annahme.

21 Separabler Abschluss

Seie L und N Körpererweiterungen von K. Wir schreiben $L \preceq N$, falls es einen Körperhomomorphismus $L \to N$ über K gibt. Dieser ist dann natürlich injektiv und wir können, falls wir einen solchen gewählt haben L als Unterkörper von N auffassen. Aber wir warnen davor, dass dies nicht eindeutig ist und natürlich verschiedene Wahlen von Körperhomomorphismen moglich sind (die Anzahl ist nach Satz 11.6 durch $[L : K]$ nach oben beschränkt). In der Tat definiert $\preceq$ eine Ordnung auf der Menge der Isomorphieklassen von Körpererweiterungen von K.
Es folgt ausserdem aus Satz 13.13, dass man jede endlich Körpererweiterung L/K zu einer normalen Körpererweiterung N/K erweitern kann, indem man einfach den Zerfällungskörper aller Minimalpolynome bildet (oder alternativ die Menge aller Nullstellen von Minimalpolynomen in einem gewählten algebraischen Abschluss $\overline{L}$ wählt). Dies nennt man auch manchmal einen normalen Abschluss von L.

Proposition 21.1. *Sei L/K eine Körpererweiterung.*

1. *Falls L/K endlich ist, so ist sie genau dann separabel, wenn für jede normale Erweiterung N/K mit $L \preceq N$ gilt*

$$|\operatorname{Hom}_K(L, N)| = [L : K] \ .$$

2. *Seien x und y in L separabel. Dann auch $x + y$ und xy in L.*

3. *Die Menge $L^{\text{sep}} \subseteq L$ aller in L separablen Elemente eine Körpererweiterung von K. Ausserdem ist jede von separablen Elementen erzeugte Körpererweiterung separabel.*

4. *Seien $K \to L$ und $L \to E$ separabel. Dann ist auch E/K separabel.*

Proof. Angenommen L/K ist separabel. Mit Induktion über $[L : K]$ können wir annehmen, dass $L = K(\alpha)$ für eine separables Element α. Dann sind aber die Nullstellen des Minimalpolynoms verschieden und liefern verschiedene Abbildungen $L \to N$ sodass Gleichheit gilt. Falls umgekehrt L/K nicht separabel ist gibt es $\alpha \in L$ mit nicht separablem Minimalpolynom. Dann gibt

es weniger als $[K(\alpha) : K]$ Morphismen $K(\alpha) \to N$ und damit auch weniger als $[L : K]$-Abbildungen von $L \to N$ aufgrund der Gradformel (siehe Beweis von Satz 11.6). Um (2) zu beweisen können wir zu der endlichen Erweiterung $K(x, y) \subseteq L$ übergehen. Dann gilt aber, dass es für jedes N mit $K(x, y) \preceq N$- genau $[K(x) : K]$-Morphism/en $K(x) \to N$ und damit $[L : K]$-Morphismen $L \to N$ gibt und die Erweiterung ist separabel. (3) wird von (2) impliziert.
Um (4) zu sehen, können wir annehmen, dass E/L und E/K endlich sind. Dann gilt aber für jede normale Erweiterung N/K, dass

$$|\operatorname{Hom}_K(E, N)| = |\coprod_{\operatorname{Hom}_K(L,N)} \operatorname{Hom}_L(E, N)| = \sum_{\operatorname{Hom}_K(L,N)} |\operatorname{Hom}_L(E, N)|$$

N ist natürlich auch normal über K, sodass diese Summe gleich $[E : L] \cdot [L : K] = [E : K]$ ist. □

Korollar 21.2. *Sei $f \in K[x]$ separabel und E/K eine Zerfällungskörper. Dann ist E/K separabel (und natürlich normal).*

Nun diskutieren wir das separable Analog zum algebraischen Abschluss.

Definition 21.3. *Ein Körper heisst separabel abgeschlossen, wenn jedes separable Polynom in Linearfaktoren zerfällt.*

Satz 21.4. *Für eine Körpererweiterung E/K sind äquivalent:*

1. *E ist separabel abgeschlossen und E/K ist separabel.*
2. *E ist Zerfällungskörper aller separabler Polynome in $K[x]$.*
3. *E ist separabel abgeschlossen und für jede Körpererweiterung L/K mit L separabel abgeschlossen existiert ein Morphismus $E \to L$ über K ("die kleineste separabel abgeschlossene Erweiterung von K").*
4. *Es gilt*
$$E \cong \{x \in \overline{K} \mid x \text{ separabel über } K\}$$
für einen algebraischen Abschluss $\overline{K}$.
5. *E/K ist separabel und für jede weitere separable Erweiterungen L/K existiert ein Morphismus $L \to E$ über K ("die grösste separable Erweiterung von K").*

Proof. (1) ⇒ (2): Sei E separabel abgeschlossen. Wir wollen zeigen, dass es ein Zerfällungskörper ist. Natürlich zerfallen alle separablen Polynome aus $K[x]$ über E. Für jeden echten Unterkörper $E' \subseteq E$ über dem alle separablen Polynome aus $K[x]$ zerfallen gibt es es Element $x \in E \setminus E'$. Dieses hat ein separables Minimalpolynom. Also muss x bereits in E' enthalten sein, da sonst das Minimalpolynom nicht zerfallen würde.
(2) ⇒ (3): Der zweite Teil ist klar aufgrund der universellen Eigenschaft, da alle separablen Polynome aus $K[x]$ in $L[x]$ zerfallen. Um zu sehen, dass E separabel abgeschlossen ist wähle ein separables irredduzibles Polynom $f \in E[x]$

mit zugehöriger Körpereweiterung E'. Dann ist $E;/K$ separabel, also jedes Element $e \in E'$ separabel über $E[x]$ und damit bereits im Zerfällungskörper enthaltemn/
(3) $\Rightarrow$ (4) : Sei $\overline{K}$ ein algebraischer Abschluss. Wir wählen eine Abbildung $E \to \overline{K}$ nach (3), da algebraisch abgeschlossene Körper auch separabel abgeschlossen sind. Das Bild besteht aus separablen Elementen (da die Minimalpolynome erhalten werden) und is somit in der Menge der separablen Elemente enthalten, wir haben also das E isomorph zu einem Unterkörper von $\overline{K}^{\text{sep}}$ ist. Da aber E/K separabel ist folgt gleichheit.
(4) $\Rightarrow$ (5): Klar aus der schwachen universellen Eigenschaft des algebraischen Abschlusses
(5) $\Rightarrow$ (1): Sei $f \in E[x]$ ein irreduzibles, separables Polynom mit zugehöriger Körpererweiterung E'/E. Diese ist separabel, also auch separabel über E, also auch separabel über K. Wir bekommen also eine Abbildung $L \to E$ über K. Die beiden kompositionen sind dann also Isomorphismen und f zerfällt schon über K. □

Definition 21.5. *In diesem Fall sagen wir E ist ein separabler Abschluss von K und wir schreiben $E = K^{\text{sep}}$. Dieser existiert natürlich nach dem vorangegangen Satz und ist natürlich wieder bis auf nicht-kanonische Isomorphie eindeutig.*

Beispiel 21.6. Falls K Charakteristik 0 hat oder perfekt von Charakteristik p ist so stimmen $\overline{K}$ und K^{sep} überein. Im Allgemeinen ist dies nicht der Fall, zum Beispiel für $\mathbb{F}_p(t)$ sind sie verschieden (da es eine nicht-separable Körpererweiterung gibt). Konkret gilt, dass

22 Galois Erweiterungen

Wir erinnern daran, dass für eine Gruppenwirkung einer Gruppe G auf einem Körper E (d.h durch Körperautomorphismen) die Fixpunkte E^G eine Unterkörper von E sind.

Satz 22.1. *Sei E/K eine Körpererweiterung mit $G := \text{Aut}_K(E)$. Dann sind äquivalent:*

1. *E ist normal und separabel*
2. *E/K ist algebraisch und die kanonische Abbildung $K \to E^G$ ist ein Isomorphismus.*
3. *Jedes $e \in E$ ist algebraisch über K und es gilt*

$$\min_K(e) = \prod_{\beta \in Ge} (x - \beta)$$

wobei Ge der Orbit der G-Wirkung auf E ist. [6].

[6] Teil des Statements ist die endlichkeit des Orbits Ge sodass die Formel Sinn macht

Falls E/K endlich ist, sind diese Bedingungen auch noch äquivalent zu

4. *Es gilt $|G| = [E : K]$.*

Proof. (1) $\Rightarrow$ (2): wir haben immer eine Inklusion $K \subseteq E^G$, da es sich um einen Morphismus von Körpern handelt. Sei also ein Element in $e \in E$ gegeben welches nicht in K liegt. Wir müssen einen Körperautomorphismus $\varphi : E \to E$ finden sodass $\varphi(e) \neq e$. Wir betrachten dazu zunächst eine Abbildung

$$K(e) \to E$$

welche e nicht fix lässt, indem wir feststellen, dass das Minimalpolynom von e mindestens Grad 2 hat und damit zwei verschiedene Nullstellen in E. Diese Abbildung können wir dann induktv zu E forsetzen indem wir induktiv Elemente adjungieren (alle auftretenden Minimalpolynome haben mindestens eine Nullstelle in E).
(2) $\Rightarrow$ (3): Sei $f(x) = \min_K(e)$ das Minimalpolynom. Offensichtlich ist e Nullstelle von f. Somit is auch jedes ge für $g \in G$ ebenfalls eine Nullstelle von f s und daher gibt es nur endlich viele solche Elemente und das Polynom

$$\prod_{\beta \in Ge} (x - \beta)$$

teil das Minimalpolynom. Weiter gilt, dass dieses Polynom Koeffizienten in $E^G = K$ hat. Somit muss es gleich dem Minimalpolynom sein (da beide normiert sind).
(3) $\Rightarrow$ (1): Klar, da das Polynom separabel ist und daher das Minimalpolynom jedes Elementes separabel ist und über K zerfällt.
Sei nun E/K endlich und normal und separabel. Dann folgt aus Proposition 21.1(1) sofort die Gleichheit

$$|G| = |\mathrm{End}_K(E)| = [E : K]$$

Falls umgekehrt diese Gleichheit gilt, so folgt, dass

$$|G| = [E : K] \geq [E : E^G] \geq |G|$$

weil $G \subseteq \mathrm{Aut}_{E^G}(E)$. Also folgt mit der Gradformel, dass $[E^G : K] = 1$ und somit $K = E^G$. □

Definition 22.2. *Falls für eine Körpererweiterung E/K die äquivalenten Bedinungen erfüllt sind so nennen wir sie eine* Galoiserweiterung *und $G =: \mathrm{Gal}(E/K)$ die Galoisgruppe.*

23 Die Galois Korrespondenz

Wir erinnern, dass eine Galoiserweiterung eine Körpererweiterung $K \to E$ ist die normal und separabel ist. Die Galoisgruppe ist dann $G = \mathrm{Aut}_K(E) = \mathrm{Gal}(L/K)$. Eine äquivalente Beschreibung davon Galois zu sein ist, dass E/K algebraisch ist und die Abbildung $K \to E^G$ ein Isomorphismus ist.

Beispiel 23.1. 1. Die Erweiterung $\mathbb{C}/\mathbb{R}$ ist Galois mit Galoisgruppe $\mathbb{Z}/2$.

2. Die Körpererweiteungen $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist Galois, denn es gilt

$$|\operatorname{Aut}_{\mathbb{Q}} \mathbb{Q}(\zeta_n)| = |(\mathbb{Z}/n)^\times| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \ .$$

   Die Galois Gruppe ist $(\mathbb{Z}/n)^\times$.

3. Sei $\mathbb{F}_{p^n}$ ein endlicher Körper mit p^n-Elementen. Dann ist die Erweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ Galois mit Galoisgruppe $\mathbb{Z}/n$.

4. Der separable Abschluss $K \to K^{\text{sep}}$ ist eine Galois Erweiterung. Zum Beispiel ist $\overline{\mathbb{Q}}/\mathbb{Q}$ Galois. Der algebraischen Abschluss ist im Allgemeinen nicht Galois, da er nicht separabel ist. Der separable Abschluss ist die "grösste" Galois Erweiterung von K, da jede andere Galois Erweiterung darin eingebettet werden kann (tatsächlich sogar jede separable Erweiterung). Im Allgmeinen ist die Galoisgruppe von K^{sep} sehr kompliziert, da die Erweriterung fast immer unendlich ist.

5. Sei E/K Galois. Dann ist für jeden Zwischenkörper $K \subseteq L \subseteq E$ die Erweiterung E/L ebenfalls Galois: sie ist normal, denn E ist Zerfällungskörper von Polynomen über E, erst recht also über L. Sie ist separabel, denn jedes Minimalpolynom über L teilt das Minimalpolynom über K.

6. In der Situation von (5) ist L natürlich nicht notwendigerweise Galois über K. Sie ist natürlich separabel, aber muss nicht normal sein, zum Beispiel $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Lemma 23.2 (Artin)**.** *Sei H eine endliche Untergruppe von* $\operatorname{Aut}(E)$ *für einen Körper E. Dann gilt, dass*

$$[E : E^H] \leq |H| \ .$$

Proof. Setze $K := E^H$. Sei $G = \{g_1 = 1, g_2, ..., g_n\}$ und seien $e_1, ..., e_m$ Elemente von E für $m > n$. Wir wollen zeigen, dass diese Elemente linear abhängig sind. Dazu betrachten wir die $(n \times m)$-Matrix

$$A = \begin{pmatrix} g_1(e_1) & ... & g_1(e_m) \\ g_2(e_1) & ... & g_2(e_m) \\ ... & ... & ... \\ g_n(e_1) & ... & g_n(e_m) \end{pmatrix}$$

über E. Diese hat wegen $m > n$ einen nicht-trivialen Kern. Wir nehmen eine Lösung $(c_1, ..., c_m)$ im Kern mit der minimal Möglichen Anzahl an nicht-null Einträgen c_i. Wir können obda annehmen, dass $c_1 \neq 0$ und dann durch Multiplikation mit einem Skalar in E, dass $c_1 \in K$. Wenn wir zeigen können, dass alle c_i in K sind, sind wir fertig, da wir eine Linearkombination der e_i gefunden haben (als erste Zeile der Matrix). Falls $c_i \notin K$ für ein i, dann existiert ein g_j mit $g_j(c_i) \neq c_i$. Wir wenden nun g_j-Elementeweise an: Durch anwenden von g_j

auf die Gleichungen und unter Benutzung, dass $\{g_1, ..., g_n\} = \{g_j g_1, ..., g_j g_m\}$ finden wir, dass

$$(g_j(c_1), g_j(c_2), .., g_j(c_n)) = (c_1, g_j(c_2), ..., g_j(c_n))$$

ebenfalls im Kern der Matrix liegt. Dann ist die Differenz der beiden Vektoren nicht-null (der i-te Eintrag) ist nicht-null, aber der erste Eintrag ist null im Widerspruch zur Minimalität von c. □

Korollar 23.3. *Sei H eine endliche Gruppe die auf einem Körper E mittels Körperautomorphismen operiert, d.h. mittels eines Gruppenhomomorphismus $\rho : H \to \mathrm{Aut}(E)$. Dann ist E/E^H eine endliche Galois-Erweriterung mit Galoisgruppe $\mathrm{Im}(\rho)$.*

Proof. Wir können obdA annehmen, dass ρ injektiv ist, indem wir H durch $\mathrm{Im}(\rho)$ ersetzen. Dann ist $[E : E^H]$ endlich. Ausserdem haben wir für $G = \mathrm{Aut}_{E^H}(E)$, die Inklusionen:

$$E^H \subseteq E^G \subseteq E^H$$

(die erste weil G Automorphismen über E^H sind und die zweite weil $H \subseteq G$) sodass Gleicheit herrscht und somit ist E/E^H eine Galoiserweiterung mit Galoisgruppe G. Wir haben aber auch

$$|H| \leq |G| = [E : E^H] \leq |H|$$

(wobei das letzte aus Artin's Lemma folgt) also sind die Gruppen gleich. □

Satz 23.4 (Hauptsatz der Galois Theorie)**.** *Sei E/K eine endliche Galoiserweiterung mit Galoisgruppe G.*

1. *Dann ist die Abbildung*

$$\begin{aligned} \{\textit{Zwischenkörper von } E/K\} &\to \{\textit{Untergruppen von } G\} \\ L &\mapsto \mathrm{Aut}_L(E) \end{aligned}$$

   eine Bijektion mit inverser Abbildung

$$\begin{aligned} \{\textit{Untergruppen von } G\} &\to \{\textit{Zwischenkörper von } E/K\} \\ H &\mapsto E^H \end{aligned}$$

   Diese Bijektion ist Inklusionsumkehrend.

2. *Unter dieser Bijektion entsprechen die Normalteiler $H \subseteq G$ genau den Zwischenkörpern L die normal über K sind, also selbst Galois. Für eine solche Zwischen-Galois Erweiterung $K \subseteq L \subseteq E$ gilt dann, dass*

$$\mathrm{Gal}(L/K) \cong G/H \ .$$

Proof. Für einen Zwischenkörper $K \subseteq L \subseteq E$ ist E/L Galois (siehe Beispiel 23.1). Also gilt, dass

$$L = E^{\mathrm{Gal}(E/L)} .$$

Umgekehrt sei $H \subseteq G$ eine Untergruppe. Dann gilt nach dem Korollar 23.3 $\mathrm{Gal}(E/E^H) = G$ sodass die Umgekehrte Gleichheit folgt. Das zeigt den ersten Teil.
Für den zweiten Teil stellen wir fest, das für $g \in G$ und $H \subseteq G$ offensichtlich gilt

$$g(E^H) = E^{gHg^{-1}}$$

wie man sofort nachrechnet. Insbesondere ist L^H genau dann invariant unter der Galoisgruppe G, wenn H normal ist. Andererseits ist die Körpererweiterung E^H/K genau dann normal, wenn E^H invariant unter G ist:

> für $e \in E$ ist das Minimalpolynom von $e \in E$ gegeben durch
>
> $$\min_K(e) = \prod_{\beta \in Ge} (x - \beta) .$$
>
> Dieses zerfällt in E^H offensichtlich genau dann, wenn $ge \in E^H$ für alle $g \in G$.

Sei nun $H \subseteq G$ normal. Dann hat die Abbildung

$$G \to \mathrm{Gal}(E^H/K)$$

Kern H (das sind genau die Morphismen die E^H fix lassen) und faktorisiert zu einer injektiven Abbildung

$$G/H \to \mathrm{Gal}(E^H/K) .$$

Nun folgt dass dies ein Isomrotphismus ist aus der Gleichheit

$$|G/H| = |G|/|H| = [E : K]/[E : E^H] = [E^H : K]$$

und wir sind fertig. □

Beispiel 23.5. Wir wollen die Galoiskorrespondenz exemplarisch anhand der Galoiserweiterung $[\mathbb{Q}(\zeta_7); \mathbb{Q}]$ verstehen. Das Element $\zeta_7 = \exp(2\pi i/2)$ hat Minimalpolynom $x^6 + x^5 + ... + x + 1$. Also ist dies eine Erweiterung von Grad 6 mit Galoisgruppe

$$G = (\mathbb{Z}/7)^\times = \langle 3 \rangle = \{\sigma \mid \sigma^6 = 1\} \qquad \text{denn die Potenzen sind } 3, 2, 6, 4, 5, 1, 3, ...$$

Der Erzeuger σ entspricht dem Körperautomorphismus $\sigma : \mathbb{Q}(\zeta_7) \to \mathbb{Q}(\zeta_7)$ der ζ_7 auf ζ_7^3 abbildet. Die einzigen Untergruppen von

$$G \cong \mathbb{Z}/6 = \mathbb{Z}/2 \times \mathbb{Z}/3$$

sind also neben den trivialen die Untergruppen erzeugt von σ^2 (eine Untergruppe der Ordnung 3) und σ^3 (eine Untergruppe der Ordnnung 2). Dies sind ebenfalls Normalteiler.

Es gilt $\sigma^2(\zeta_7) = \zeta_7^2$ und die Fixpunkte sind eine Körpererweiterung

$$L_1 = (\mathbb{Q}(\zeta_7))^{\sigma^2}$$

von Grad 2 entsprechen. Es gilt offensichtlich, dass σ^2 das Element

$$\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$$

festlässt und dieses Element nicht rational sind (sonst hätte σ ein kleiners Minimalpolynom). Also gilt, dass

$$L_1 = \mathbb{Q}(\alpha)$$

Dies ist eine Erweiterung von Grad zwei, kann als durch adjungieren einer Wurzel erhalten werden (rechnen Sie die mal aus!). Die Galoisgruppe $\langle\sigma\rangle/\langle\sigma^2\rangle$ wirkt durch $\sigma(\alpha) = \zeta_7^3 + \zeta_7^6 + \zeta_7^5 = \overline{\alpha}$, also durch komplexe Konjugation. Weil damit auch

$$\alpha - \sigma(\alpha) = \sqrt{-7}.$$

fest bleibt, haben wir auch

$$L_1 = \mathbb{Q}(\sqrt{-7}) \ .$$

Analog sieht man, dass der Fixkörper

$$L_2 = (\mathbb{Q}(\zeta_7))^{\sigma^3}$$

von Ordnung 3 ist und dieser enthält $\zeta_7 + \zeta_7^6 = 2\mathrm{Re}(\zeta_7) = 2\cos(2\pi i/7)$. Da dies nicht rational ist und L_2 keine weiteren Unterkörper enthält gilt also, dass

$$L_2 = \mathbb{Q}(\cos(2\pi i/2))$$

mit Galoisgruppe der Ordnung 3 is (erzeugt von σ).

Wir wollen nun die Galois Korrespondenz als Äquivalenz von Kategorien schreiben. Dazu sei $\mathrm{Field}_{/K}^{\preceq E} \subseteq \mathrm{Field}_{/K}$ die volle Unterkategorie aller Körpererweiterungen L/K die sich nach E einbetten lassen (d.h. sodass $L \preceq E$ über K).

Satz 23.6 (Kategorielle Version)**.** *Sei E/K eine endliche Galois Erweiterung mit Galois Gruppe G. Dann ist der Funktor*

$$\begin{aligned}\left(\mathrm{Field}_{/K}^{\preceq E}\right)^{\mathrm{op}} &\to \mathrm{Set}^{BG} \\ L &\mapsto \mathrm{Hom}_K(L, E)\end{aligned}$$

eine Äquivalenz auf die volle Unterkategorie der transitiven G-Mengen. Hier wirkt G auf $\mathrm{Hom}_K(L, E)$ durch die Wirkung auf E, also

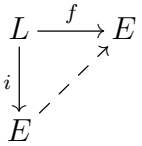
$$(g \cdot f)(l) = g(f(l)) \ .$$

24 Die Äquivalenz von Kategorien

Proof. Zunächst müssen wir zeigen, dass der Funktor tatsächlich in transitiven G-Mengen landet. Dazu sei $L \in \mathrm{Field}_{/K}^{\preceq E}$ und wir fixieren eine Abbildung $i : L \to E$ die wir der einfachheit halber als Inklusion annehmen, also $L \subseteq E$. Für jede weitere Abbildung

$$f' : L \to E$$

finden wir dann eine Fortsetzung



denn um dies zu garantieren müssen wir zeigen, dass die Minimalpolynome $\min_L(e)$ für jedes $e \in E$ zerfallen, d.h. $f(min_L(e))$ muss über E zerfallen. Es gilt aber, dass $\min_L(e)$ ein Teiler von $\min_K(e)$ ist und letzteres ist gleich $f(\min_K(e))$ zerfällt also aufgrund der Normalität von E/K. Also zerfällt auch das erste. Dies impliziert aber, dass die Menge $\mathrm{Hom}_K(L, E)$ als G-Menge transitiv ist. Der Stabilisator von i ist gegeben durch alle Automorphismen in G die L festlassen, also die Galoisgruppe von E über L.
Um zu zeigen, dass der Funktor eine Äquivalenz ist konstruieren wir nun einen Umkehrfunktor

$$\mathrm{Set}_{\mathrm{trans}}^{BG} \to \mathrm{Field}_{K/}^{\preceq E}$$

der eine G-Menge X sendet auf die Menge der G-äquivarianten Abbildungen $\mathrm{Hom}_G(X, E)$. Dies wird ein kommutativer Ring mittels punktweiser Addition und Multiplikation und enthält K als konstante Abbildungen. Wir behaupten, dass es sogar ein Körper ist. Dazu stellen wir fest, dass X isomorph zu G/H ist. Nach Wahl eines solchen Isomorphismus ist aber

$$\mathrm{Hom}_G(X, E) \cong \mathrm{Hom}_G(G/H, E) = E^H$$

und dies ist offfensichtlich ein Unterkörper von E (die beiden Ringstrukturen stimmen per Konstruktion überein). Wir müssen nun zeigen, dass die beiden Funktoren inverse zueinander sind. Dazu betrachten wir die Komposition

$$\mathrm{Set}_{\mathrm{trans}}^{BG} \to \mathrm{Set}_{\mathrm{trans}}^{BG}$$

welche X auf $\mathrm{Hom}_K(\mathrm{Hom}_G(X, E), E)$ schickt. Es gibt eine kanonische Abbildung von G-Mengen

$$X \to \mathrm{Hom}_K(\mathrm{Hom}_G(X, E), E) \qquad x \mapsto \mathrm{ev}_x$$

Diese ist wohldefiniert und natürlich wie man sofort nachrechnet (machen!). Wir behaupten, dass es ein Isomorphismus ist. Dazu dürfen wir annehmen $X = G/H$ und in dem Fall ist es die kanonische Abbildung

$$G/H \to \mathrm{Hom}_K(E^H, E)$$

welche ein Isomorphismus ist (nach der Berrechnung am Anfang). Die andere Komposition von Funktoren funktioniert analog und das beweist den Satz. □

Korollar 24.1. *Für zwei Unterkörper $L, L' \subseteq E$ assoziiert mit Untergruppen $H, H' \subseteq G$ gilt*

$$\mathrm{Hom}_K(L, L') \cong \mathrm{Hom}_G(G/H', G/H) = \{[g] \in G/H \mid gHg^{-1} \subseteq H'\} \ .$$

Beispiel 24.2. Betrachte wieder $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ mit Galoisgruppe $G = \mathbb{Z}/3 \times \mathbb{Z}/2$. Wir hatten die beiden Zwischenkörper $\mathbb{Q}(\sqrt{-7})$ (assoziert zur Untergruppe $\mathbb{Z}/3$) und $\mathbb{Q}(\cos(2\pi/7))$ (assoziiert zur Untergruppe $\mathbb{Z}/2$) gefunden. Nun wollen wir die Morphismen dazwischen bestimmen: es gilt, dass

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-7}, \mathbb{Q}(\cos(2\pi/7)) &\cong \mathrm{Hom}_G(G/(\mathbb{Z}/2, G/(\mathbb{Z}/3)) \\ &= \emptyset\end{aligned}$$

und analog

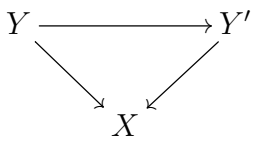
$$\mathrm{Hom}_{\mathbb{Q}}((\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\zeta_7)) = \mathrm{Hom}_G(G, G/(\mathbb{Z}/3)) = \mathbb{Z}/2$$

Wir wollen nun sehen in welcher Art und Weise die Äquivalenz von Kategorien die klassische Galois Korrespondenz verallgmeinert. Aus dem Beweis wissen wir, dass der Funktor ein Unterkörper $K \subseteq L \subseteq E$ auf die G-Menge G/H für $H = \mathrm{Gal}(E/L)$ schickt. Allerdings ist H dadurch nur bis auf Konjugation festgelegt. Insbesondere bekommen wir durch den Funktor eine Bijektion:

$$\begin{aligned}&\{\text{Isoklassen von Körpererweiterungen } L/K \text{ die } \preceq E \text{ sind }\} \\ &\quad \cong \{\text{Konjugationsklassen von Untergruppen von } G\}\end{aligned}$$

Dies ist ein etwas anderes Statement als die Klassische Galoisäquivalenz. Wir können aber auch diese formal zurückgewinnen wie folgt:

Definition 24.3. *Sei $\mathcal{C}$ eine Kategorie und $X \in \mathcal{C}$ wir definieren die Überkategorie $\mathcal{C}_{/X}$ deren Objekte bestehen aus Paaren $Y \in \mathcal{C}$ mit einem Morphismus $Y \to X$. Ein Morphismus in $\mathcal{C}_{/X}$ von $Y \to X$ nach $Y' \to X$ is gegeben durch einen Morphismus $Y \to Y'$ sodass das Diagram*



kommutiert. Komposition ist Komposition von Morphismen. Analog definieren wir die Unterkategorie $\mathcal{C}_{X/}$.

Jede Äquivalenz von Kategorien $F : \mathcal{C} \simeq \mathcal{D}$ induziert für $X \in \mathcal{C}$ eine Äquivalenz

$$\mathcal{C}_{/X} \simeq \mathcal{D}_{/F(X)} \ .$$

Beispiel 24.4. Für $\mathcal{C} = \mathrm{Field}^{\preceq E}_{/K}$ ist $\mathcal{C}_{/E}$ äquivalent zu der Kategorie induziert von dem Poset der Zwischenkörper zwischen K und E.
Für $\mathcal{C} = \mathrm{Set}^{BG}_{\mathrm{trans}}$ ist $\mathcal{C}_{G/}$ äquivalent zum Poset der Untergruppen von G.
Die Äquivalenz von Kategorien induziert also eine Äquivalenz von Kategorien zwischen diesen beiden Kategorien, insbesondere eine Bijektion zwischen den beiden Posets. Dies ist die klassische Galoiskorrespondenz.

25 Anwendungen

Wir erinnern an die Sätze 2.8 und Korollar 10.7 die über Konstruierbarkeit des regelmäßigen n-Ecks gehen. Wir haben gesehen, dass für die Konstruierbarkeit des n-Ecks $\varphi(n)$ eine 2er Potenz sein muss. Wir wollen nun die Umkehrung zeigen:

Satz 25.1 (Gauss)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist, also wenn wenn n von der Form $n = 2^k \cdot p_1 \cdot ... \cdot p_k$ für paarweise verschiedene Fermat'sche Primzahlen gilt.*

Proof. Wir müssen nur noch zeigen, dass falls $\varphi(n)$ eine 2er Potenz ist $\zeta_n \in \mathbb{C}$ konstuierbar ist. Dazu reicht es nach Satz 2.8 zu beweisen, dass $\mathbb{Q}(\zeta_n)$ durch iteriertes adjungieren von Quadratwurzeln ensteht, oder äquivalent (nach Lemma 2.11) durch iterierte Grad 2 Erweiterungen von $\mathbb{Q}$. Nach der Galois Korrespondenz entsprechen diese Zwischenkörper genau Untergruppen von $G = (\mathbb{Z}/n)^\times$. Weil dies ein 2-Gruppe ist haben wir aber ein solches System

$$\{e\} \subseteq G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G \ .$$

□

Satz 25.2 (Satz vom primitiven Element)**.** *Für jede endliche, separable Erweiterung L/K existiert ein element $a \in L$ sodass $L = K(a)$ (gennant primitves Element). Ausserdem hat jede solche Erweiterung nur endlich viele Zwischenkörper.*

Proof. Wir betrachten die normale Hülle E/K. Diese ist ebenfalls separabel, also eine Galoiserweirterung. die Unterkörper on L sind dann in 1-1 Beziehung zu den Untergruppen von $\mathrm{Gal}(E/K)$ die $\mathrm{Gal}(E/L)$ enthalten. Also gibt es nur endlich viele. Jetzt müssen wir die Existenz eines primitiven Elementes zeigen. Wir machen dies unter der Zusatzannahme, dass K unendlich viele Elemente hat. Den endlichen Fall kann man von Hand erledigen (ausgelassen). Jetzt wählen wir $a \in E$ sodass der Grad des Minimalpolynoms von a maximal ist, i.e. $K(a)$ maximalen Grad über E hat. Falls ein $x \in E \setminus K(u)$ existiert so finde $\lambda_1 \neq \lambda_2$ in K mit

$$K(u + \lambda_1 x) = K(u + \lambda_2 x) = L_1$$

Dann ist

$$(u + \lambda_1 x) - (u + \lambda_2 x) = (\lambda_2 - \lambda_1)x \in L_1$$

also auch $x, u \in L_1$ im Widerspruch zur Maximalität von u. □

Korollar 25.3. *Dier endlichen Galoiserweiterungen eines von K sind genau die Zerfällungskörper von sepearablen, irreduzibles Polynomen $f \in K[x]$.*

Proof. Einerseits ist wie wir gesehen haben jeder solche Zerfällungskörper eine Galoiserweiterung. Umgekehrt existiert zu jeder Galoiserweiterung E/K ein primitives Element $a \in E$. Dann ist $E \cong K[a]/\min_K(a)$ und weil E normal ist zerfällt das Polynom über E. Also ist E Zerfällungskörper von $\min_K(a)$. □

Abschließend wollen wir auch noch einen Beweis des Fundamentalsatzes der Algebra geben. Dazu brauchen wir ein paar Hilfsmittel:
Wir brauchen zunächst ein paar Hillfsmittel aus der Gruppentheorie:

Satz 25.4 (Cauchy)**.** *Sei G eine endliche Gruppe mit $p||G|$ für eine Primzahl p. Dann existiert in G ein Element der Ordnung p .*

Proof. Betrachte die Menge

$$X = \{(g_1, .., g_p) \in G^p \mid \prod g_i = 1\}$$

Dann ist $|X| = |G^{p-1}|$ durch p teilbar. Es gibt eine zyklische Wirkung von $\mathbb{Z}/p$ auf X. Wir haben also, dass die Fixpunktmenge $X^{\mathbb{Z}/p}$ Kardinalität durch p teilbar hat, aufgrund von Satz 18.18. Elemente in dieser Menge sind aber genau Gruppenelemente $x \in G$ mit $x^p = 1$. Da diese Menge 1 enthält, also nicht-leer ist muss sie mindestens ein weiteres Element enthalten. □

Dieser Satz wird von folgendem Satz verallgemeinert:

Satz 25.5 (1. Sylowsatz)**.** *Sei G eine endliche Gruppe sodass p^n teilt $|G|$ für p prim. Dann existiert eine Untergruppe $U \subseteq G$ der Ordnung n.*

Proof. Wir Beweisen den Satz durch Induktion nach n. Falls p die Ordnung von $Z(G)$ teilt so existiert nach dem Satz von Cauchy ein Untergruppe $U \subseteq Z(G)$ der Ordnung p. Diese ist normal in G. Wir betrachten die Projektion

$$\pi : G \to G/U$$

Nach Induktionsannahme gibt es in G/U eine Untergruppe der Ordnung p^{n-1} sodass $\pi^{-1}(U)$ die gesuchte Gruppe ist. Falls p nicht die Ordnung des Zentrums teilte, so muss wegen der Zerlegung

$$|G| = |Z(G)| + \sum |Gx|$$

mit x Repräsentanten von allen ein-elementigen Orbits ein Orbit $Gx = G/H$ existieren mit Ordnung prim zu p. Das Bedeutet aber, dass die Untergruppe H eine durch p^n teilbare Ordnung hat und wir finden per Induktionsannahme eine Untergruppe der Ordnung p^n in H. □

26 Anwendungen 2

Definition 26.1. *Sei $|G| = p^n a$ mit a teilerfremd zu p. Dann heisst eine Untergruppe $P \subseteq G$ der Ordnung p^n eine Sylowuntergruppe von G. Diese existiert nach dem Satz.*

Satz 26.2 (2. Sylowsatz)**.** *Sei $P \subseteq G$ eine Sylowuntergruppe. Dann existiert für jede Untergruppe $H \subseteq G$ der Ordnung p^k (d.h. H ist eine p-Gruppe) ein $g \in G$ sodass $gHg^{-1} \subseteq P$. Insbesondere sind je zwei Sylowuntergruppen konjugiert (und damit isomorph als abstrakte Gruppen).*

Proof. Betrache G/P als H-Menge bezüglich Linksmultiplikation. Weil H eine p-Gruppe ist und die Ordnung von G/P teilerfremd zu p ist, hat die Wirkung einen Fixpunkt (nach Proposition 18.18), d.h. es gibt ein $g \in G$ sodass für jedes $h \in H$ gilt

$$hgP = gP$$

also $g^{-1}hg \in P$. □

Bemerkung 26.3. Es gibt auch noch einen dritten Sylowsatz (der etwas über die Anzahl der Sylowgruppen aussagt), aber wir werden diesen nicht brauchen.

Satz 26.4 (Fundamentalsatz der Algebra)**.** *Jedes nicht-konstante Polynom $f \in \mathbb{C}[x]$ hat eine Nullstelle.*

Proof. Sei $L/\mathbb{R}$ eine endliche, normale Erweiterung mit Galoisgruppe G und sei $P \subseteq G$ eine 2-Sylowgruppe mit zugehörigem Unterkörper $L^P \subseteq L$. Dann ist

$$[L : L^P] = |P|$$

und daher ist $[L^P : \mathbb{R}]$ ungerade. Für jedes $x \in L^P$ muss also das Minimalpolynom ungeraden Grad haben. Damit hat es aber schon eine Nullstelle über $\mathbb{R}$ und kann daher nicht irreduzibel über $\mathbb{R}$ sein. Also folgt $L^P = \mathbb{R}$ und somit $P = G$, also ist G eine 2-Gruppe. Nach dem Struktursatz für 2-Gruppen gibt es dann aber eine Sequenz von Zwischenkörpern

$$\mathbb{R} \subseteq L_1 \subseteq L_2 \subseteq ... \subseteq L_k = L$$

wobei jede Erweiterung die Ordnung 2 hat, also durch adjungieren einer Wurzel entsteht. Also ist L_1 bereits gleich $\mathbb{C}$ und $k = 1$, also $L = \mathbb{C}$ oder $L = \mathbb{R}$. Es folgt also, dass jede normale, algebraische Erweiterung von $\mathbb{R}$ bereits in $\mathbb{C}$ enthalten sein muss, also ist $\mathbb{C}$ der algebraische Abschluss von $\mathbb{R}$. □

Definition 26.5. *Sei $f \in K[x]$ ein Polynom sodass alle irreduziblen Faktoren separabel sind. Dann ist ein Zerfällugskörper E/K Galois und wir nennen die Galois Gruppe* $\mathrm{Gal}(E/K)$ *die Galoisgruppe von f und scheiben* $\mathrm{Gal}(f/K)$.

Wir warnen, dass die Galoisgruppe bis auf Äquivalenz eindeutig ist, aber nicht kanonisch da die Wahl eines Zerfällungskörpers involviert ist. Falls $a_1, ..., a_n$ die Nullstellen von f im Zerfällungskörper E sind, so bildet jedes Element in $\mathrm{Gal}(f/K)$ Nullstellen von f auf Nullstellen ab und induziert daher eine Permutation der Nullstellen. Die Abbildung ist dadurch natürlich auch bestimmt, da die Nullstellen den Zerfällungskörper erzeugen. Wir bekommen also eine Injektion

$$\mathrm{Gal}(f/K) \to \mathrm{Aut}_{\mathrm{Set}}(\{a_1, ..., a_n\}) = \Sigma_n \ .$$

Falls f irreduzibel ist, dann operiert $\mathrm{Gal}(f/K)$ sogar transitive auf der Menge der Nullstellen (i.A. nicht).

Bemerkung 26.6. Sei K^{sep} ein separabler Abschluss von K. Dann können wir E als Unterkörper von K^{sep} erzeugt aus den Nullstellen von f realisieren. Es folgt, dass wir $\mathrm{Gal}(f/K)$ als Quotient der Gruppe der Automorphismen

von K^{sep} realisieren können: durch Einschränkung bekommen wir einen Homomorphismus

$$\text{Aut}(K^{\text{sep}}) \to \text{Aut}(E)$$

und dieser ist surjektiv, da wir nach der schwachen universellen Eigenschaft jeden Morphismus forsetzen können. Wir haben also auch eine Abbildung

$$\text{Aut}(K^{\text{sep}}) \to \Sigma_n$$

welche als Bild die Galoisgruppe hat. Das ist die Beschreibung der Galoisgruppe die wir in der ersten Vorlesung gegeben haben.

Bemerkung 26.7. Tatsächlich besteht $\text{Gal}(f/K)$ genau aus den Permutationen σ von $\{a_1, ..., a_n\}$ für die gilt, dass für jedes Polynom $P \in K[X_1, ..., X_n]$ in n-Variablen gilt, dass $P(a_1, ..., a_n) = 0$ impliziert, dass auch $P(\sigma a_1, ..., \sigma a_n) = 0$. Dies beschreibt die Galoisgruppe ohne über abstrakte Gruppen und Körper zu sprechen und so hat Galois dies getan.

Beispiel 26.8. Betrachte das Polynom $f(x) = X^3 - 2 \in \mathbb{Q}[x]$. Dieses ist nach Eisenstein irreduzibel und hat den Zerfällungskörper

$$E := \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

da die Nullstellen von f durch $a := \sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$ und $\sqrt[3]{2}\zeta_3^2$ gegeben sind. Es gilt, dass E wegen

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq E$$

Grad 6 hat. Daher hat auch die Galoisgruppe 6 Elemente und die Injektion

$$\text{Gal}(f, \mathbb{Q}) \to \Sigma_3$$

ist eine Bijektion.

Beispiel 26.9. Betrachte das Polynom $X^4 - 2 \in \mathbb{Q}[x]$. Dieses ist nach Eisenstein irreduzibel. Dann ist

$$E = \mathbb{Q}(\sqrt[4]{2}, i)$$

ein Zerfällungskörper (da die Nullstellen gegeben sind für $a = \sqrt[4]{2}$ durch $\pm a, \pm ai$). Dieser lässt sich schreiben als

$$\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$$

sodass E den Grad 8 über $\mathbb{Q}$ hat. Es gilt auch

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq E$$

sodass aus Gradgründen wieder $[\mathbb{Q}(a, i) : \mathbb{Q}(i)] = 4$ und daher ist f auch das Minimalpolynom von a über $\mathbb{Q}(i)$.
Wir haben nun Morphismen

$$\sigma : E \to E \qquad i \mapsto i, a \mapsto ai$$

von Ordnung 4 und

$$\tau : E \to E \qquad a \mapsto a, i \mapsto -i$$

von Ordnung 2. Es ist klar, dass $\tau \neq \sigma^k$ sodass die Galoisgruppe gegeben ist durch

$$\mathrm{Gal}(f, \mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

Wenn wir dies als Untergruppe der Permutationen von $a, ai - a, -ai$ auffassen, so bekommt man folgende geometrische Beschreibung: Zeichne ein Quadrat mit Eckpunkten $a, ai - a, -ai$ zeichnen, so liefert σ eine Drehung um 90 Grad und τ eine Spiegelung and der Diagonalen. Die Gruppe, die man so erhält ist die sogennante Diedergruppe D_4 aller Symmetrien des Vierecks. Wir sehen in dem Beispiel auch, dass die Galoisgruppe eines Polynoms kleiner sein kann als die Symmetrische Gruppe.

Definition 26.10. *Sei $f \in K[x]$ ein Polynom. Die Gleichung $f = 0$ heisst durch Radikale auflösbar, wenn seine Nullstellen durch die algebraischen Operationen Addition, Subtraktion, Multiplikation, Division und das Ziehen n-ter Wurzel erhalten werden. Genauer, wenn es eine Kette von Körpererweiterungen*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n = E$$

gibt, sodass K_{i+1} aus K_i durch adjungieren einer n-ten Wurzel entsteht und sodass f über E in Linearfaktoren zerfällt (äquivalent, dass E einen Zerfällungskörper von f enthält).

Definition 26.11. *Eine endliche Gruppe G heisst auflösbar, wenn es eine Folge von Untergruppen*

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G$$

gibt sodass G_i normal in G_{i+1} ist und Index von Primzahlordnung hat (äquivalent, der Quotient ist zyklisch von Primzahlordnung).

Satz 26.12 (Galois)**.** *Sie K ein Körper der Charakteristik 0 und $f \in K[x]$. Dann ist die Gleichung $f = 0$ genau dann durch Radikale lösbar wenn die Galoisgruppe $\mathrm{Gal}(f, K)$ auflösbar ist.*

Wir werden diesen Satz am Ende der Vorlesung beweisen (wenn die Zeit reicht) und zunächst einmal anwenden. Dazu wollen wir den Begriff der auflösbaren Gruppen etwas untersuchen.

Beispiel 26.13. Die Gruppe Σ_2 ist offensichtlich auflösbar. Wir sehen also sofort, dass jedes Polynom 2.ten Grades durch Radikale gelöst werden kann.

Beispiel 26.14. Die Gruppe Σ_3 ist auflösbar, denn wir haben

$$\{e\} \subseteq A_3 = \mathbb{Z}/3 = \langle(123)\rangle \subseteq \Sigma_3$$

mit Quotienten $\mathbb{Z}/3$ und $\mathbb{Z}/2$. Man sieht ausserdem leicht, dass auch alle Untergruppen von Σ_3 (also $\mathbb{Z}/2$ und $\mathbb{Z}/3$ auflösbar sind) und damit jedes Polynom 3. Grades durch Radikale aufgelöst werden kann.

Beispiel 26.15. Die Gruppe Σ_4 ist auflösbar, denn wir haben die Reihe

$$\{e\} \subseteq \mathbb{Z}/2 \subseteq \mathbb{Z}/2 \times \mathbb{Z}/2 \subseteq A_4 \subseteq \Sigma_4$$

wobei $\mathbb{Z}/2 \times \mathbb{Z}/2$ als Untergruppe von A_4 erzeugt wird von den Elementen $g = (12)(34)$ und $h = (13)(24)$. Es ist einfach zu sehen, dass diese Untergruppe $\mathbb{Z}/2 \times \mathbb{Z}/2$ ist (beide Elemente haben Ordnung 2 und kommutieren). Ausserdem ist diese Untergruppe normal. Die Quotienten haben alle die Ordnung 2.
Es wäre nun möglich alle Untergruppen anzuschauen. Stattdessen werden wir beweisen, dass Untegruppen auflösbarer Gruppen selbst auflösbar sind.

27 Auflösbare Gruppen

Satz 27.1. *Sei G eine endliche Gruppe.*

1. *Falls G auflösbar ist, so ist auch jede Untergruppe und jeder Quotient nach einem Normalteiler auflösbar.*
2. *Falls für einen Normalteiler N die Gruppen N und G/N auflösbar sind, so auch G*
3. *Abelsche Gruppen sind auflösbar*
4. *p-Gruppen sind auflösbar.*

Proof. Sei

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G$$

die Reihe die die Auflösbarkeit bezeugt. Für eine Untergruppe $U \subseteq G$ betrachten wir die induzierte Sequenz

$$\{1\} = G_0 \cap U \subseteq G_1 \cap U \subseteq G_2 \cap U \subseteq ... \subseteq G_n \cap U = U$$

Mit den Quotienten

$$(G_i \cap U)/(G_{i-1} \cap U)$$

welche Untergruppen von G_i/G_{i-1} sind und daher ebenfalls von Prim Ordnung oder 1 sind. Also ist U auflösbar.
Für eine Surjektion $p : G \to \overline{G}$ haben wir eine induzierte Sequenz

$$\{1\} = p(G_0) \subseteq p(G_1) \subseteq p(G_2) \subseteq ... \subseteq p(G_n) = \overline{G}$$

und wir finden, dass $p(G_i)$ normal in $p(G_{i-1}$ ist und erhalten eine Surjektion

$$G_i/G_{i-1} \to p(G_i)/p(G_{i-1})$$

Also ist wiederum der Quotient von Ordnung p oder trivial.
Für (2) nehmen wir Ketten

$$\{1\} = N_0 \subseteq N_1 \subseteq N_2 \subseteq ... \subseteq N_n = N$$

$$\{1\} = Q_n \subseteq Q_{n+1} \subseteq Q_{n+2} \subseteq ... \subseteq Q_m = G/N$$

wir setzen $N_i := p^{-1}Q_i$ für $i \geq n$ (note $N_n = N$ ist konsisten). Es gilt

$$N_i/N_{i-1} \cong Q_i/Q_{i-1}$$

sodass G auflösbar ist.
Sei G abelsch. Dann erhält G eine nicht-triviale Untergruppe (ausser $G = \mathbb{Z}/p$) die ein Normalteiler ist. Per Induktion nach der Gruppenordnung wissen wir, dass G/N und N auflösbar sind, also auch G.
Die letzte Aussage folgt aus dem Struktursatz für p-Gruppen Satz 18.21 (der wesentlich stärker ist). □

Korollar 27.2. *Für jedes Polynom $f \in \mathbb{Q}[x]$ von Grad ≤ 4 kann die Gleichung $f = 0$ durch Radikale gelöst werden.*

Proof. Dies folgt, da jede Untergruppe von Σ_4 auflösbar ist. □

Korollar 27.3. *Eine endliche Gruppe ist genau dann auflösbar, wenn es eine Folge*

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G$$

von Untergruppen gibt, sodass G_i normal in G_{i+1} ist und sodass die Quotienten abelsch sind (oder zyklisch).

Proof. Beide Richtungen sind klar. □

Definition 27.4. *Eine Gruppe G heisst einfach, wenn sie keine nicht-trivialen Normalteiler besitzt.*

Beispiel 27.5. Eine auflösbare Gruppe A ist genau dann einfach, wenn sie isomorph zu $\mathbb{Z}/p$ für p prim ist. Insbesondere sind dies die einzigen abelschen, einfachen Gruppen.

Satz 27.6. *Die alternierende Gruppe $A_n \subseteq \Sigma_n$ ist für $n \geq 5$ einfach, also insbesondere nicht auflösbar.*

Bevor wir den Satz beweisen zunächst eine Konsequenz:

Korollar 27.7. *Die Gruppe Σ_n ist für $n \geq 5$ nicht auflösbar, da sie A_n als Untergruppe hat.*

Nun wollen wir den Satz beweisen. Dazu zunächst etwas Terminologie: Ein 3-Zykel ist eine Permutation der form (abc) mit verschiednenen a, b, c. Wegen

$$(abc) = (ab)(bc)$$

liegt dieser in A_n.

Lemma 27.8. *A_n wird von 3-Zykeln erzeugt.*

Proof. Die Gruppe Σ_n wird von Transpositonen erzeugt, also ist jedes Element ein Produkt von solchen (inverse sind ebenfalls Transpositionen). Dieses Element liegt also in A_n genau dann, wenn wir eine Gerade Anzahl an Transpositionen haben. Insbesondere wird A_n von Produkten $(ab)(cd)$ erzeugt. Falls alle a, b, c, d verschieden sind haben wir

$$(ab)(cd) = (bcd)(abc)$$

und falls nicht so sind sie entweder gleich also Invers zu einander oder wir haben einen 3-Zykel □

Lemma 27.9. *In A_n für $n \geq 5$ sind alle 3-Zykel zueinander konjugiert.*

Proof. Wir zeigen, dass jeder 3-Zykel zu (123) konjugiert ist. Dazu sei der 3-zykel (abc) gegeben. Wähle d, e verschieden zu abc und Wir betrachten eine Permutation $\tau \in \Sigma_n$ mit

$$\tau(1) = a, \tau(2) = b, \tau(3) = c$$

Falls τ ungerade ist ersetzen wir τ durch $\tau \circ (45)$, können also obda annehmen, dass $\tau \in A_n$ liegt. Dann ist aber

$$\tau^{-1}(abc)\tau = (123) \ .$$

□

Beweis von Satz 27.6. Sie $N \subseteq A_n$ nicht-trivialer Normalteiiler und $\sigma \in N$ ein Element $\sigma \neq 1$ mit maximlaler Anzahl an Fixpunkten (für die Wirkung auf $\{1, ..., n\}$). Wir wollen zeigen, dass σ ein 3-Zykel ist. Dann folgt aber, dass alle 3-Zylel in N liegen und damit $N = A_n$.

1. Wir schreiben σ in Zykelschreibweise. Angenommen es kommen nur Transpositionen vor (äquivalent: alle Bahnen der induzierten $\mathbb{Z}$-Wrikung auf $\{1, .., n\}$ haben höchtens 2 Elemente). Dann hat σ obda die Form

   $$\sigma = (12)(34)...$$

   da es gerade ist. Betrachte $\tau = (345)$. Dann ist

   $$\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$$

   Fixpunkte von σ ungleich $1, 2, 3, 4, 5$ sind auch Fixpunkte von σ'. Ausserdem sind $1, 2$ jetzt Fixpunkte von σ'. Insbesondere hat σ' mehr Fixpunkte als σ (es könnte sein, dass 5 ein Fixpunkt von σ war und keiner mehr ist, aber das macht nichts). Ausserdem ist

   $$\sigma'(3) = 5$$

   sodass $\sigma' \neq 1$. Widerspruch.

2. Also existiert mindestens ein längerer Zykel in σ der Länge ≥ 3, obda $\sigma(1) = 2$, $\sigma(2) = 3$. Falls σ ein 3-Zyklel ist sind wir fertig. Sonst muss σ mindestens ein weiteres Element bewegen und daher, weil σ ungerade ist mindestens zwei weitere Elemente die keine Fixpunkte sind, obda 4 und 5. Setze nun $\tau = (345)$ und betrachte

$$\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$$

Jeder Fixpunkt von σ ist auch ein Fixpunkt von σ' und es gilt $\sigma'(2) = 2$ und $\sigma'(3) = 4$. Also hat σ' weniger Fixpunkte als σ und ist nicht die Identität, im Widerspruch zur Minimalitätsannahme.

□

Korollar 27.10. *Ein Polynom $f \in \mathbb{Q}[x]$ mit Galoisgruppe Σ_5 kann nicht auflösbar sein.*

Wir werden im kommenden Kapitel explizite Polynome finden, zum Beispiel $f(x) = 24x^5 - 30x^4 + 5$. t

28 Nicht-auflösbare Polynome

Nach Galois' Satz und der Tatsache, dass Σ_n für $n \geq 5$ nicht auflösbar ist, wollen wir nun ein Polynom 5.ten Grades über $\mathbb{Q}$ konstruieren, welches Galoisgruppe Σ_5 hat. Dieses kann dann nicht durch Radikale aufgelöst werden.

Lemma 28.1. *Sei $U \subseteq \Sigma_p$ eine Untergruppe für p prim, die eine Transposition und ein Element der Ordnung p enthält. Dann gilt $U = \Sigma_p$.*

Proof. Ein Element $\sigma \in \Sigma_p$ der Ordnung p muss bereits ein p-Zykel sein, denn wenn wir es in Zykelschreibweise schreiben

$$(a_1..a_n)(b_1...b_k)...$$

mit disjunkten Zykeln hat es als Ordnung ein Teiler des produktes der Zykellängen, also niemals p falls es kein p-Zykel ist. Wir nehmen an, dass die Transposition obda (12) ist und der Zykel

$$\sigma = (1a_1a_2...a_p)$$

Eine Potenz von σ bildet 1 auf 2 ab und ist auch noch ein p-Zykel. Also können wir auch obda annehmen, dass

$$\sigma = (123...p)$$

nach erneuten umbennen. Es gilt nun

$$(i, i+1) = \sigma^i(12)\sigma^{-i}$$

für jedes i. Also enthält U auch alle diese Elemente und ist daher ganz Σ_p. □

Proposition 28.2. *Sei $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom 5.ten Grades mit genau drei rellen Nullstellen. Dann gilt* $\mathrm{Gal}(f, \mathbb{Q}) = \Sigma_5$.

Proof. Sei E ein Zerfällungskörper von f und $a \in E$ eine Wurzel von f. Dann gilt

$$[\mathbb{Q}(a) : \mathbb{Q}] = 5$$

da das Polynom irreduzibel ist. Aufgrund der Gradformel teilt also 5 die Ordnung der Galoisgruppe und wir finden somit ein Element der Ordnung 5. Ausserdem ist die Komplexe Konjugation ein Element der Galoisgruppe, da sie die beiden komplexen Nullstellen vertauscht und den Rest festlässt. Sie gibt also eine Transposition der beiden Nullstellen. Es folgt nun, dass die gesamte Galoiisgruppe gleich Σ_5 ist. □

Beispiel 28.3. Betrachte das Polynom $f(x) = 2x^5 - 10x + 5$. Es gilt $f(-2) < 0, f(-1) > 0, f(1) < 0, f(2) > 0$ sodass wir drei Nullstellen dazwischen haben. Die Ableitung $f'(x) = 10x^4 - 10 = 10(x^4 - 1)$ hat genau die zwei reelle Nullstellen ± 1 sodass das Polynom f keine doppelten reellen Nullstellen und keine weiteren Nullstellen hat. Aufgrund des Eisensteinkriteriums für $p = 5$ ist das Polynom irreduzibel. Also nach der Proposition gilt, dass die Galoisgruppe $\mathrm{Gal}(f/\mathbb{Q}) = \Sigma_5$ und damit können die Nullstellen nicht durch Radikale aufgelöst werden.

Warnung 28.4. *Ein anderes Polynom von Grad 5 mit Galoisgruppe Σ_5 ist $x^5 - 5x^3 + 4x - 1$ (wir werden dies hier nicht beweisen), aber dieses Polynom hat 5 reelle Nullstellen. Also sind die Bedingungen der Proposition 28.2 nicht notwendig.*

29 Adjungieren von Wurzeln

In diesem Kapitel wollen wir sogennante Kummer Erweiterungen studieren. Dazu brauchen wir zunächst etwas Vorarbeit.

Lemma 29.1. *Jede abelsche Gruppe G ist das Produkt ihrer p-Sylow Untergruppen.*

Proof. Seien $p_1, .., p_n$ die Primteiler von $|G|$ und $P_i \subseteq G$ die p_i-Sylow Untergruppen, diese existieren nach dem ersten Sylowsatz und sind eindeutig nach dem zweiten, da G abelsch ist. Wir haben nun einen Gruppenhomomorphismus

$$\prod P_i \to G \qquad (p_1, .., p_n) \mapsto \prod p_i$$

Weil die Ordnung der p_i paarweise teilerfremd ist, ist der Homomorphismus injektiv, also eine Bijektion, da Urbild und Bild gleich viele Elemente haben. □

Satz 29.2. *Sei K eine Körper und $G \subseteq K^\times$ eine endliche Untergruppe der Multiplikativen Gruppe $(K^\times, \cdot)$. Dann ist G zyklisch.*

Proof. Nach dem Lemma und dem chinesischen Restsatz können wir oBdA annehmen, dass G eine p-Gruppe ist. Sei $b \in G$ ein Element maximaler Ordnung. Dann sind

$$1, b, b^2, ..., b^{\mathrm{ord}(b)-1}$$

verschiedene Wurzeln des Polynoms $x^{\mathrm{ord}(b)} - 1 \in K[x]$, also sind dies alle Wurzeln. Für ein $c \in G$ gilt aber jetzt, dass $\mathrm{ord}(c) \leq \mathrm{ord}(b)$, also weil G eine p-Gruppe ist $\mathrm{ord}(c) | \mathrm{ord}(b)$. Also ist c ebenfalls eine Nullstelle von $x^n - 1$ und damit in $\langle b \rangle$. Also ist G zyklisch. □

Korollar 29.3. *Die Gruppe $\mathbb{F}_{p^n}^\times$ ist zyklisch.*[7]

Man kann die Einheitswurzelgruppen für beliebige Körper K betrachten:

$$\mu_n(K) = \{z \in K \mid z^n = 1\} \subseteq K^\times$$

Es ist klar, dass $\mu_n(K)$ endlich ist, denn das Polynom $x^n - 1$ kann über K höchstens n-Nullstellen haben. Die Kardinalität ist also sogar $\leq n$. Es kann aber passieren, dass so kleiner ist. Zum Beispiel kann die Kardinatlität in einem endlichen Körper K nicht größer als $|K| - 1$ sein. Es gilt aber nach obigem Satz trotzdem, dass die Gruppe der Einheitswurzeln zyklisch ist.

Betrachte nun über einem Körper K das Polynom $f(x) = x^n - a \in K[x]$ für $a \neq 0$. Falls in K gilt $n \neq 0$ so ist dieses separabel, da $f'(x) = nx^{n-1}$ nur von x geteilt wird und $f(x)$ offensichtlich nicht. Anderenfalls ist es nicht separabel. Insbesondere impliziert die Annahme, dass ein Körper n-verschiedene Einheitswurzeln hat also, dass $n \neq 0$ in K gilt. Falls dies gilt können wir die Einheitswurzeln natürlich einfach adjungieren (äquivalent den Zerfällungskörper von $x^n - 1$ bilden) und bekommen so eine Erweiterung $K \to K'$ die Galois ist und die wir für $K = \mathbb{Q}$ intensiv untersucht haben. Mit ähnlichen Methoden kann man dies nun für beliebige Körper tun indem man die Gruppen der Einheitswurzeln genauer untersucht (die Galoisgruppe ist dann stets eine Untergruppe von $(\mathbb{Z}/n)^\times$).
Beispielsweise hat jeder Körper der Charakteristik $\neq 2$ zwei verschiedene 2.te Einheitswurzeln. Wir wollen nun Lemma 2.11 verallgemeinern .

Satz 29.4. *Sei K eine Körper der n-verschiedene n-te Einheitswurzeln enthält.*

1. *Für $a \neq 0$ ist jeder Zerfällungskörper von $x^n - a$ eine Galoiserweiterung mit zyklischer Galoisgruppe von Ordnung die n teilt.*

2. *Alle Galoiserweiterungen E/K mit zyklischer Galoisgruppe von Ordnung n enstehen durch Adjunktion einer n-ten Wurzel zu K.*

Proof. Sei E ein solcher Zerfällungskörper und y eine Nullstelle von $x^n - a$. Dann sind alle Nullstellen gegeben durch $y \cdot \zeta_i$ wobei $\zeta_i \in \mu_n(K)$ die Einheitswurzeln sind. Also folgt, dass $E = K(a)$ und die Abbildung

$$\mathrm{Gal}(E/K) \to \mu_n(K) \qquad f \mapsto f(a)/a$$

[7]Daraus kann man einfach den fehlenden Teil im Beweis von Satz 25.2 ergänzen.

ist injektiv. Damit ist die Galoisgruppe einer Zyklischen Gruppe zyklisch.

Zu 2: Sei E/K Galois mit Galoisgruppe $G = \langle\sigma\rangle$ der Ordnung n. Die Eigenwerte der K-linearen Abbildung

$$\sigma : E \to E$$

sind dann n-te Einheitswurzeln, da $\sigma^n = \mathrm{id}$ (σ ist sogar diagonalisierbar). Tatsächlich sieht man einfach, dass die Eigenwerte eine Untergruppe $U \subseteq \mu_n(K)$ bilden, da für Eigenvektoren $v, w \in E$ gilt, dass vw ebenfalls Eigenvektor zum Produkt der Eigenwerte ist. Wir behaupten sogar, dass U sogar die ganze Gruppe ist. Falls nicht wäre U zyklisch von Ordnung $d < n$, also die Eigenvektoren von σ nur d-te Einheitswurzeln. Also hat σ^dnur den Eigenwert 1 und ist diagonalisierbar, also $\sigma^d = \mathrm{id}$ was ein Widerspruch ist.

Insbesondere existiert für jede Einheitswurzel ein Eigenvektor. Für einen Erzeuger ζ von $\mu_n(K)$ gibt es also einen Eigenvektor $a \in E$ sodass

$$\sigma(a) = \zeta \cdot a$$

Es folgt

$$\sigma(a^i) = \zeta^i \cdot a$$

und damit sind die a^i linear unabhängig als Eigenwerte zu verschiendenen Eigenvektoren. Also $E = K(a)$ und a ist eine n-te Einheitswurzel. □

Lemma 29.5. *Sei E/K Galois mit Galoisgruppe G.*

1. *Sei $K \subseteq L \subseteq L' \subseteq E$. Dann ist die Erweiterung $L \to L'$ selbst Galois genau dann, wenn die assozzierte Untergruppe H' normal in H ist. In diesem Fall gilt $H'/H = \mathrm{Gal}(L'/L)$.*

2. *Für jedes L mit $K \subseteq L \subseteq E$ ist der normale Abschluss $\overline{L}$ der kleineste Unterkörper der L enthält und abgeschlossen unter der G-Wirkung ist.*

Proof. 1) Betrachte E als Galoiserweiterung von L mit Galoisgruppe $H' = \mathrm{Gal}(E/L)$. Dann ist L' eine Zwischenerweiterung die zur Untergruppe H gehört und die Behauptung folgt aus der gewöhnlichen Galoiskorrespondenz.
2) Wir haben gesehen, dass eine Erweiterung $L \subseteq E$ genau dann normal ist, wenn sie abgeschlossen unter der G-Wirkung ist. Daraus folgt alles. □

Beweis von Galois' Satz 26.12. Wir führen den Beweis im für uns relevanten Fall $K = \mathbb{Q}$, der Allgemeine Fall geht analog.
Angenommen $f = 0$ ist durch Radikale auflösbar, dann wählen wir eine Kette von Körpererweiterungen

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n = E$$

wobei $K_i = K_{i-1}(a_i)$ mit $a_i^{n_i} \in K_i$. Wir fassen E' als Teilmenge von $\mathbb{C}$ auf, also $a_i \in \mathbb{C}$ und

$$E = \mathbb{Q}(a_1, a_2, ..., a_n) \ .$$

mit $a_i^{n_i} \in \mathbb{Q}(a_1, .., , a_{n-1})$. Wir adjungieren zusätzlich eine primitive k-te Einheitswurzel ζ_k für $k = \prod n_i$, betrachten also

$$E' = \mathbb{Q}(\zeta_k, a_1, a_2, ..., a_n)$$

Weiterhin bilden wir den normalen Abschluss $E' \subseteq \overline{E} \subseteq \mathbb{C}$. Dieser ist Galois mit Galoisgruppe $G = \{1, \sigma_1, \sigma_2, ..., \sigma_k\}$ und es gilt

$$\overline{E} = \mathbb{Q}(\zeta_k, a_1, \sigma_1(a_1), \sigma_2(a_1), ..., a_2, \sigma_1(a_2), ..., a_n, \sigma_1(a_n), ..., \sigma_k(a_n))$$

nach dem Lemma. Wir adjungieren nun die Elemente der Reihe nach:

$$\zeta_k, a_1, \sigma_1(a_1), \sigma_2(a_1), ..., a_2, \sigma_2(a_2), ...$$

und erhalten so einen Turm von Körpererweiterungen. Es gilt jeweils, dass $\sigma(a_i)^{n_i}$ in der vorherigen liegt. Also ist jede dieser Erweiterungen eine Erweiterung Galois mit zyklischer Galoisgruppe. Nach der Galoiskorrespondenz bekommen wir eine assoziierte Kette von Untergruppen

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G \ .$$

sodass G_i normal in G_{i+1} ist und die Quotienten zyklisch sind. Also ist G auflösbar.
Sei umgekehrt G auflösbar. Wir betrachte E als Unterkörper von $\mathbb{C}$ und adjungieren eine primitive n-te Einheitswurzel, also $E(\zeta_n)$.
Wir bekommen dann eine Kette von Körpererweitetungen

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq ... \subseteq K_i = E$$

sodass $K_i \to K_{i+1}$ Galois mit zyklischer Galoisgruppe ist. Wenn wir eine Wurzel adjungieren sind die Erweiterungen

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) = K_0(\zeta_n) \subseteq K_1(\zeta_n) \subseteq ... \subseteq K_i(\zeta_n)$$

immernoch Galoiserweiterungen mit zyklischer Galoisgruppe. Also durch adjungieren von Wurzeln erhalten. □